資安SIEM境遇 - Fortinet讓校園擁有毫不妥協的安全防護

Jarvis Lee 李尚峰
Fortinet 台灣區技術顧問
ljarvis@fortinet.com

現今資安與網維面臨的挑戰

不僅需要防護型資安解決方案，還需要建立早期預警系統

太多供應商
資訊難統整

大量日誌與告警
關聯分析困難

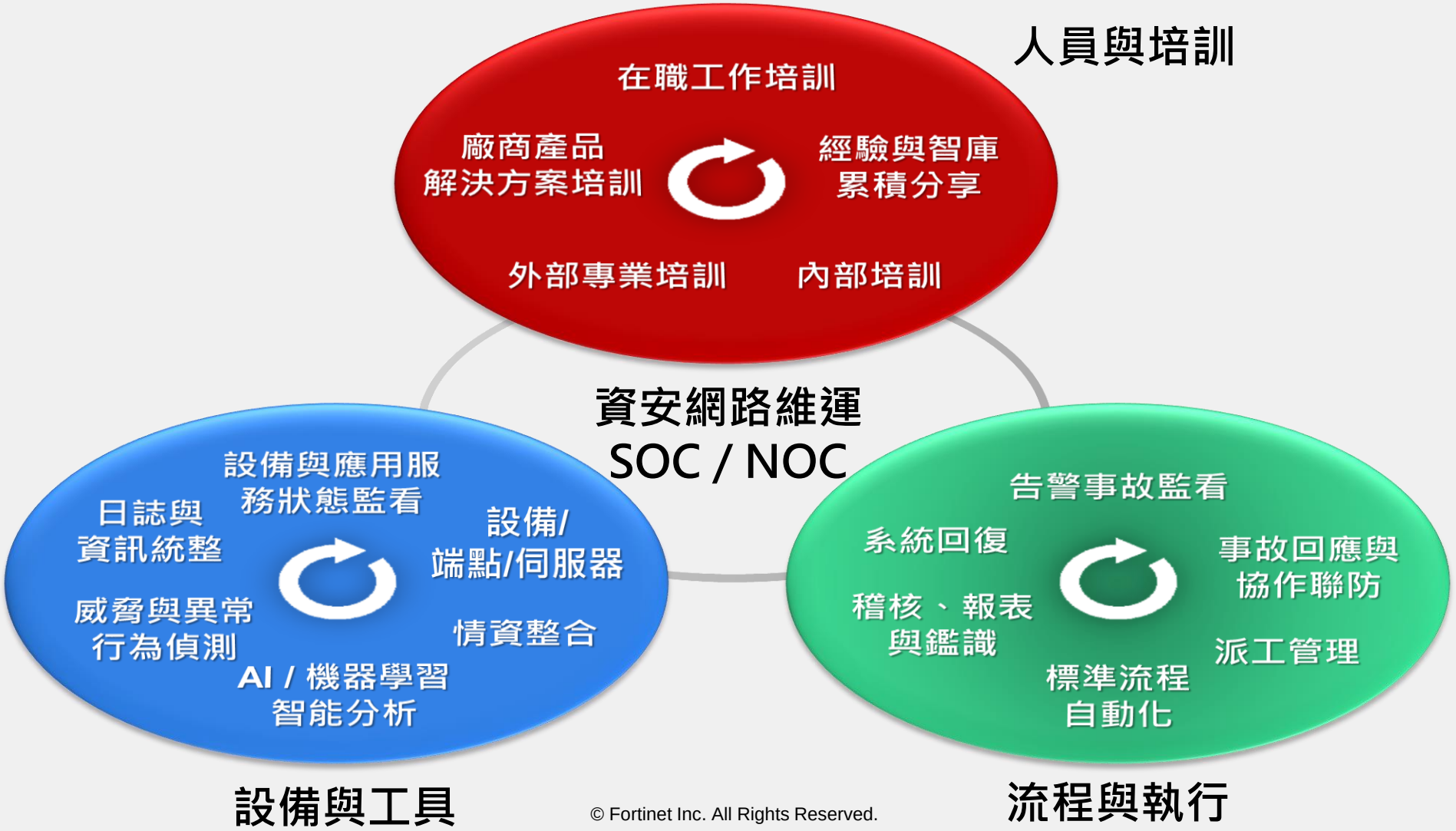
手動回應緩慢
費工耗時易出錯

缺乏有經驗
的人員

管理複雜導致
高維運成本

資安網維控管三重奏

導入好的設備與解決方案、簡單易用、標準化作業流程

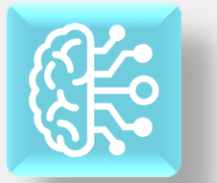


導入 AI 與機器學習，加速進階威脅偵測

AI 驅動的安全防護深入產品 DNA

基於網路資訊流
Network-Based

FortiSandbox



FortiNDR
(aka FortiAI)

基於日誌與記錄
Log-Based

FortiSIEM

基於終端行為模式
Endpoint-Based

FortiEDR

FortiGuard Lab.
Global Threat Intelligence Services

基於資安情資服務
TIS-Based

FortiSIEM 您維運管理的好幫手

資料統整、威脅偵測、維運監看、事故回應一氣呵成

標準化事故回應作業流程

- 內建派工管理系統，方便告警事故通報、分流、追蹤和管理告警事故調查與回應

告警事故協作聯防自動化

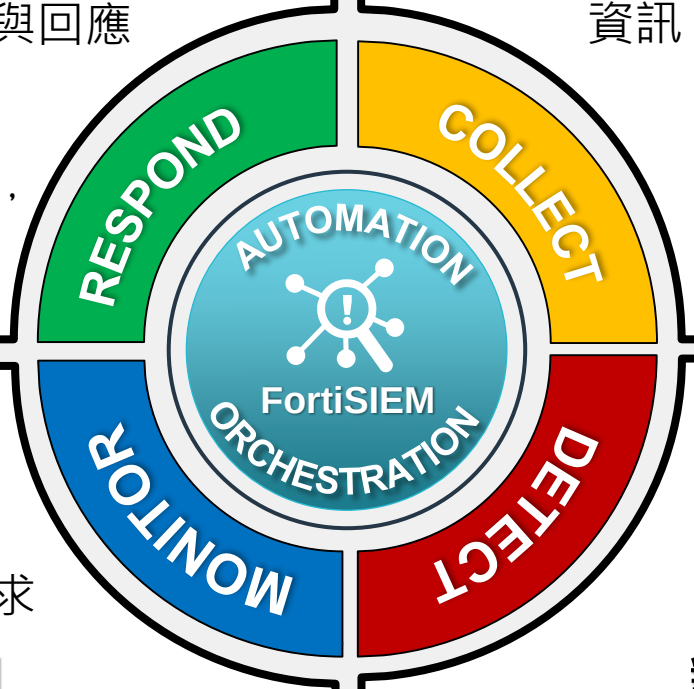
- 使用預或自定義的緩解調控腳本，手動或自動回應告警事故

多來源、多品牌日誌記錄統整與加值

- 融合 SOC 與 NOC，日誌、流量、效能資訊、應用服務記錄統整與內容加值

設備組態管理資料庫 (CMDB)

- 監看管理設備效能指標和組態
- 設備資產統整、威脅情資整合



豐富彈性的監看儀表板與報表

- 有效增進系統運作效能、可用度與資安可視性，滿足監管稽核需求

直覺式事件關聯分析，簡單易用

- Google-like 的快速資料查找方式搭配選單點擊 ，無需學習複雜的查詢語法

智能分析 (AI)，機器學習 (ML)

- 快速學習建立維運維運基準線
- 即時偵測異常行為與潛在威脅

對應 MITRE ATT&CK 資安框架

- 提供威脅情境定性分析，有效偵測進階持續性威脅 (APT)

資安 (SOC) 與網維 (NOC) 融合式分析

完善您整體資安與網維的可視性

資安日誌與資訊

NGFW / IPS / VPN

EPP/EDR

Web Application

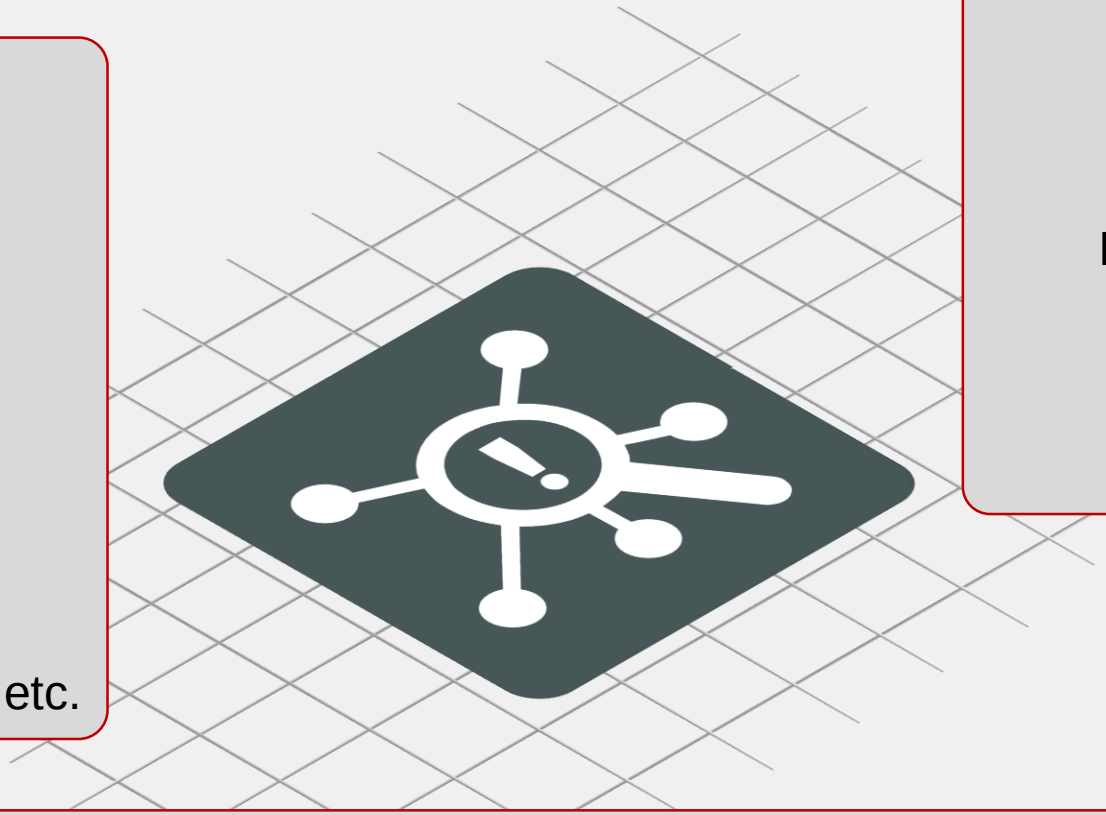
eMail System

AAA Server

Database

Traffic / Flows

Router / Switch / WLAN, etc.



設備效能監看指標

CPU

Memory

Storage

Interface Utilization

Uptime

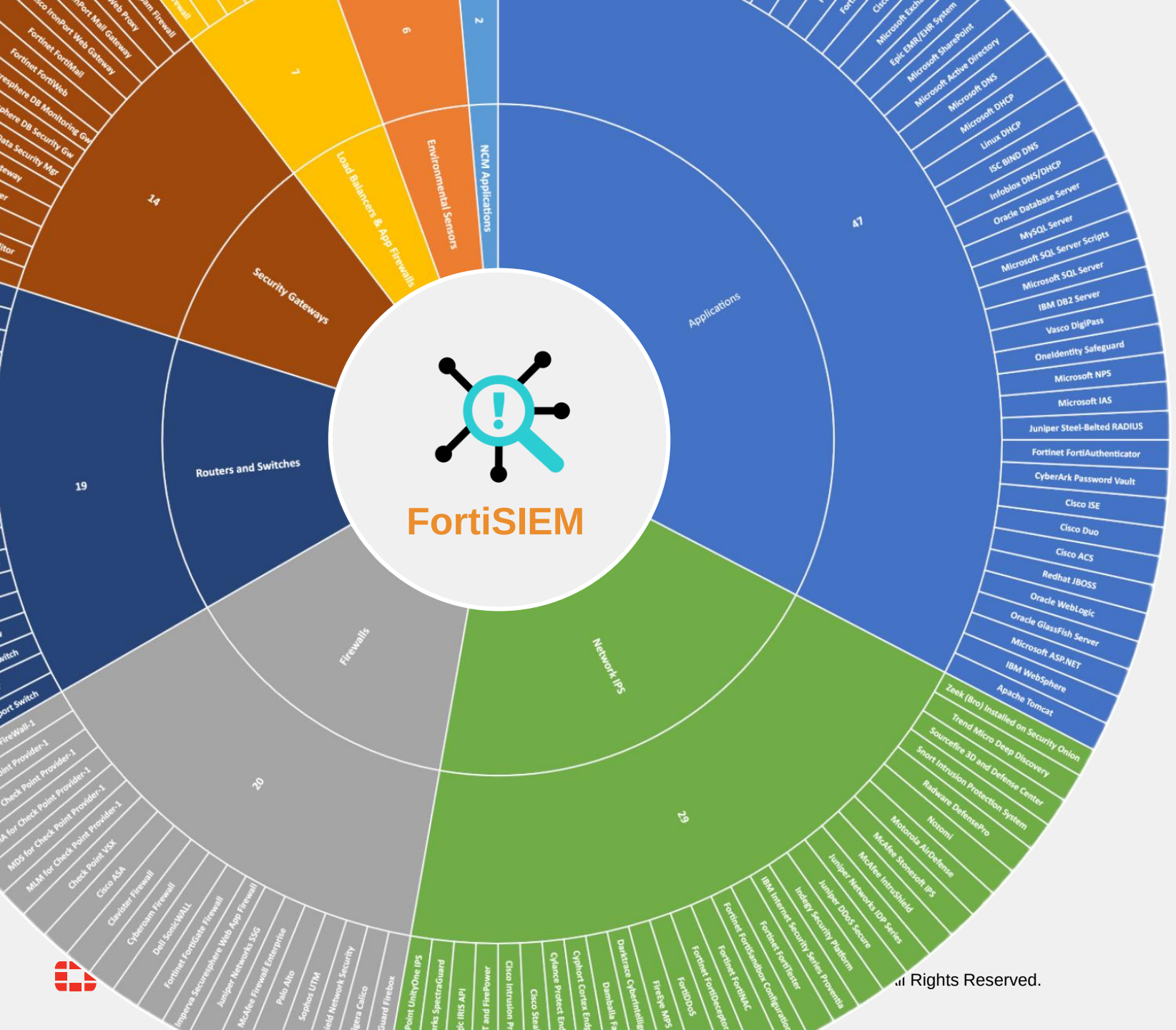
Process / Services

Configuration, etc.

融合式的資安與網維管理 (SOC & NOC)

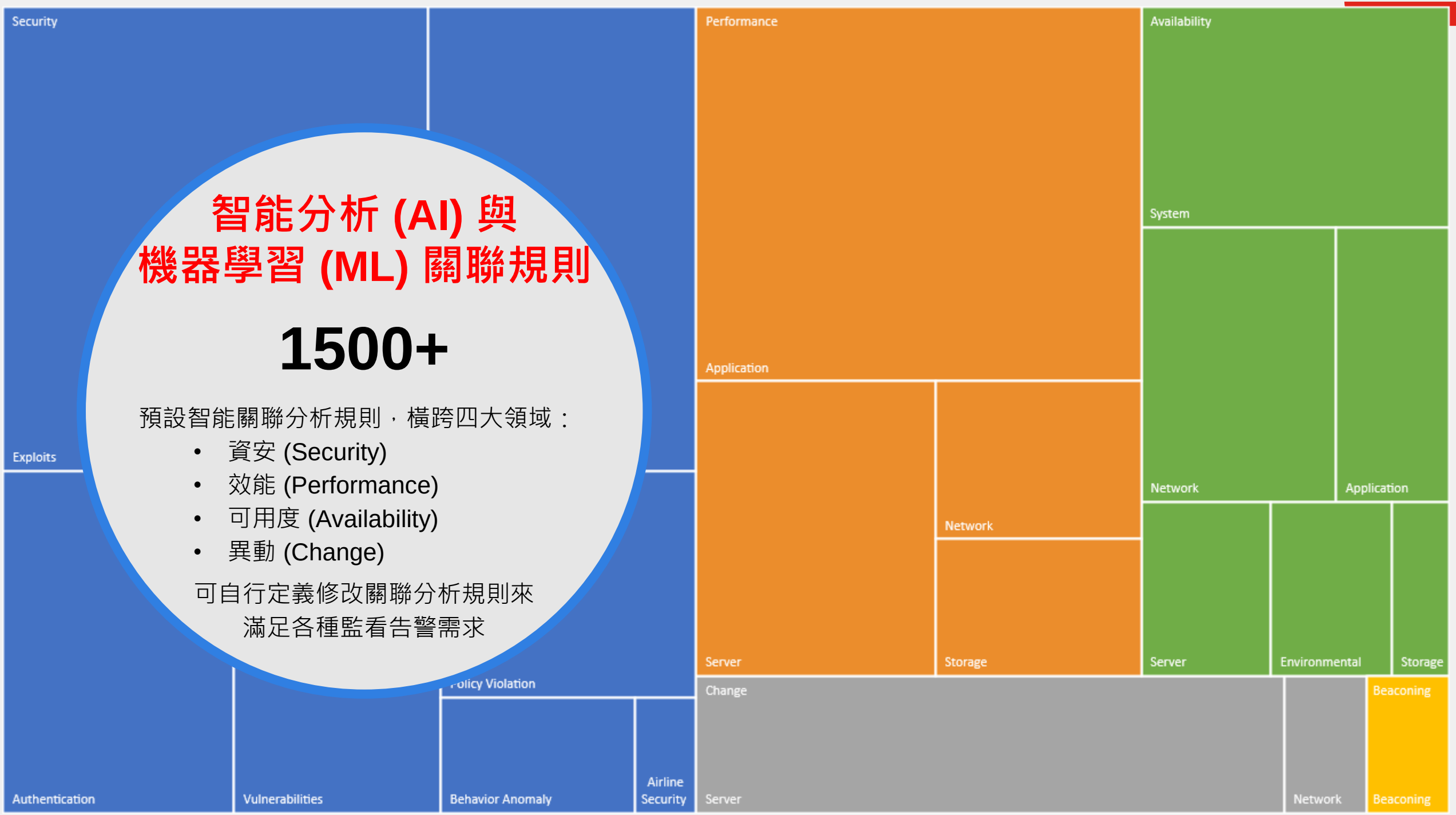
更多豐富的功能 | 更好的可視性 | 加速事故回應時間

廣泛的設備與應用服務支援



FortiSIEM 預設支援超過 400+ 種以上各式設備與應用服務

內建日誌解譯編輯器 (Parser Editor) 可支援更多設備與應用



智能分析 (AI) 與機器學習 (ML) 關聯規則

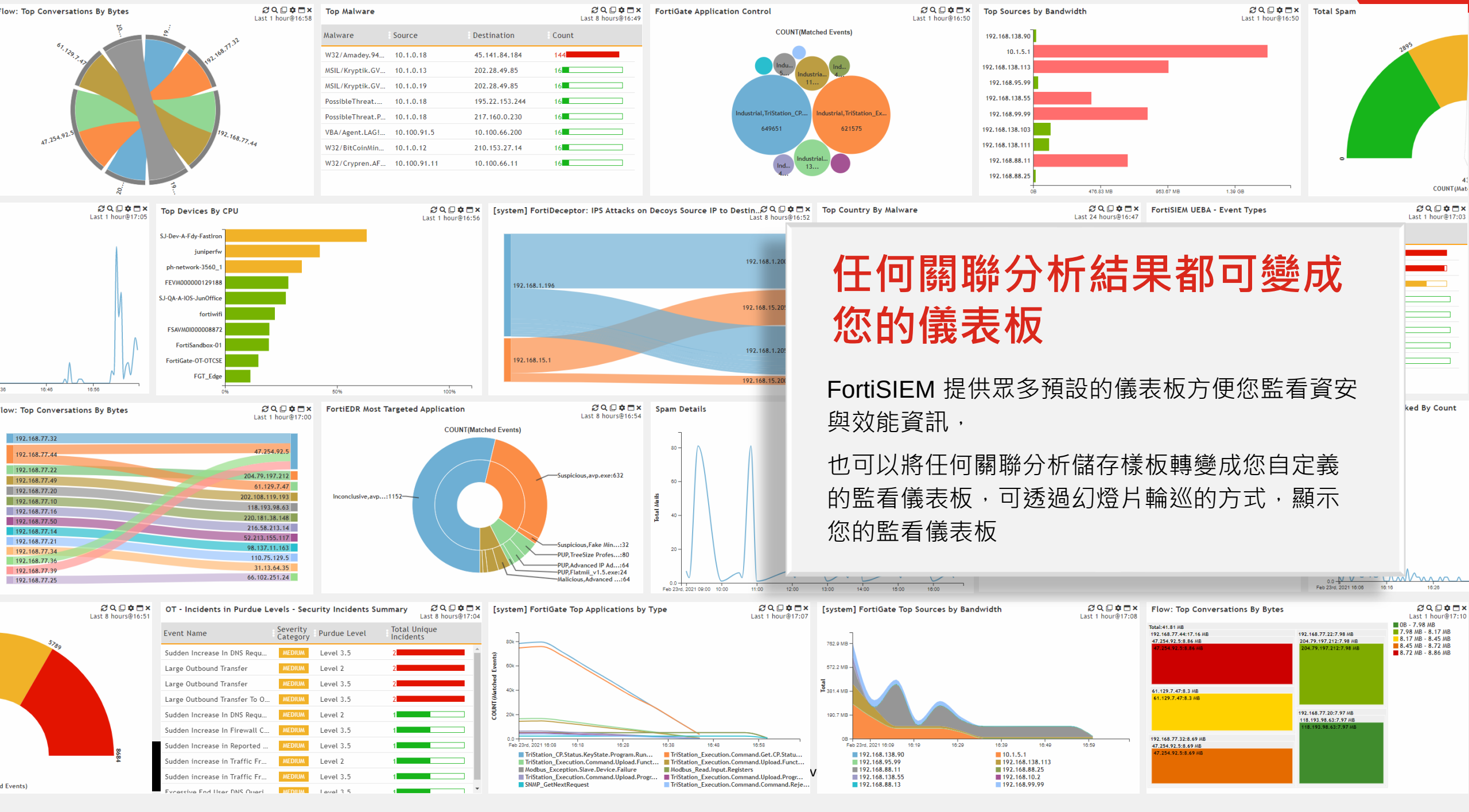
1500+

預設智能關聯分析規則，橫跨四大領域：

- 資安 (Security)
- 效能 (Performance)
- 可用度 (Availability)
- 異動 (Change)

可自行定義修改關聯分析規則來
滿足各種監看告警需求


Security
Exploits
Vulnerabilities
Performance
Application
Availability
Server
Environmental
Storage
Policy Violation
Change
Server
Network
Beaconing
Beaconing
Authentication
Vulnerabilities
Behavior Anomaly
Airline Security
內建豐富稽核與
合規性報表
3000+
預設合規性報表 (Compliance Reports)：
包括 PCI, SOX, HIPAA, FISMA, NERC, COBIT, ITIL, NIST, ISO, GLBA, GPG13, CIS, SANS, Critical Controls
內建報表客製化建構器：
3,000+ 可客製化欄位，豐富的圖表資源庫，可穿插文字與附件


Flow: Top Conversations By Bytes
Top Malware
Malware Source Destination Count
W32/Amadey.94... 10.1.0.18 45.141.84.184 144
MSIL/Kryptik.GV... 10.1.0.13 202.28.49.85 16
MSIL/Kryptik.GV... 10.1.0.19 202.28.49.85 16
PossibleThreat.... 10.1.0.18 195.22.153.244 16
PossibleThreat.P... 10.1.0.18 217.160.0.230 16
VBA/Agent.LAG!... 10.100.91.5 10.100.66.200 16
W32/BitCoinMin... 10.1.0.12 210.153.27.14 16
W32/Crypren.AF... 10.100.91.11 10.100.66.11 16
FortiGate Application Control
COUNT(Matched Events)
Industrial,TriStation_CP.... 649651
Industrial,TriStation_Ex... 621575
Top Sources by Bandwidth
192.168.138.90
10.1.5.1
192.168.138.113
192.168.95.99
192.168.138.55
192.168.99.99
192.168.138.103
192.168.138.111
192.168.88.11
192.168.88.25
Total Spam
2895
Top Devices By CPU
SJ-Dev-A-Fdy-FastIron
juniperfw
ph-network-3560_1
FEVM000000129188
SJ-QA-A-IOS-JunOffice
fortiwifi
FSAVM0I000008872
FortiSandbox-01
FortiGate-OT-OTCSE
FGT_Edge
[system] FortiDeceptor: IPS Attacks on Decoys Source IP to Destin...
192.168.1.196
192.168.15.1
Top Country By Malware
FortiSIEM UEBA - Event Types
Flow: Top Conversations By Bytes
192.168.77.32
192.168.77.44
192.168.77.22
192.168.77.49
192.168.77.20
192.168.77.10
192.168.77.16
192.168.77.50
192.168.77.14
192.168.77.21
192.168.77.34
192.168.77.36
192.168.77.39
192.168.77.25
47.254.92.5
204.79.197.212
61.129.7.47
202.108.119.193
118.193.98.63
220.181.38.148
216.58.213.14
52.213.155.117
98.137.11.163
110.75.129.5
31.13.64.35
66.102.251.24
FortiEDR Most Targeted Application
COUNT(Matched Events)
Suspicious,avp.exe:632
Inconclusive,avp...:1152
Suspicious,Fake Min...:32
PUP,TreeSize Profes...:80
PUP,Advanced IP Ad...:64
PUP,Flatmii_v1.5.exe:24
Malicious,Advanced ...:64
Spam Details
Total Mails
Feb 23rd, 2021 09:00
OT - Incidents in Purdue Levels - Security Incidents Summary
Event Name Severity Category Purdue Level Total Unique Incidents
Sudden Increase In DNS Requ... MEDIUM Level 3.5 2
Large Outbound Transfer MEDIUM Level 2 2
Large Outbound Transfer MEDIUM Level 3.5 2
Large Outbound Transfer To O... MEDIUM Level 3.5 2
Sudden Increase In DNS Requ... MEDIUM Level 2 1
Sudden Increase In Firewall C... MEDIUM Level 3.5 1
Sudden Increase in Reported ... MEDIUM Level 3.5 1
Sudden increase in Traffic Fr... MEDIUM Level 2 1
Sudden increase in Traffic Fr... MEDIUM Level 3.5 1
[system] FortiGate Top Applications by Type
COUNT(Matched Events)
TriStation_CP.Status.KeyState.Program.Run...
TriStation_Execution.Command.Upload.Funct...
Modbus_Exception.Slave.Device.Failure
TriStation_Execution.Command.Upload.Progr...
SNMP_GetNextRequest
TriStation_Execution.Command.Get.CP.Statu...
TriStation_Execution.Command.Upload.Funct...
Modbus_Read.Input.Registers
TriStation_Execution.Command.Upload.Progr...
TriStation_Execution.Command.Command.Reje...
[system] FortiGate Top Sources by Bandwidth
Total
192.168.138.90
192.168.95.99
192.168.88.11
192.168.138.55
192.168.88.13
10.1.5.1
192.168.138.113
192.168.88.25
192.168.10.2
192.168.99.99
Flow: Top Conversations By Bytes
0B - 7.98 MB
7.98 MB - 8.17 MB
8.17 MB - 8.45 MB
8.45 MB - 8.72 MB
8.72 MB - 8.86 MB
任何關聯分析結果都可變成您的儀表板
FortiSIEM 提供眾多預設的儀表板方便您監看資安與效能資訊，
也可以將任何關聯分析儲存樣板轉變成您自定義的監看儀表板，可透過幻燈片輪巡的方式，顯示您的監看儀表板

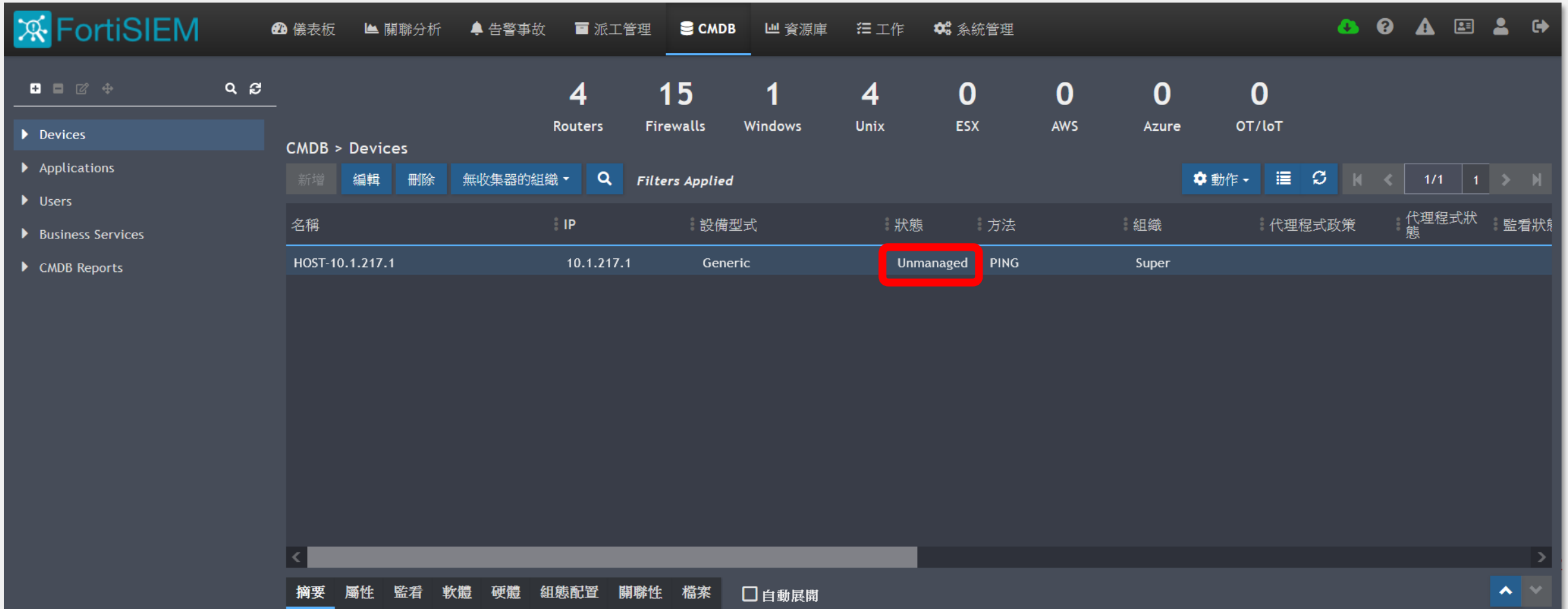
資料統整 Collect

應用範例一：設備識別與資料統整

Collect

排程自動探索環境，身分、設備與連網位置自動關聯

- 透過排程自動探索環境 (ping only discovery)，更新 CMDB 資料庫，產生 “Unmanaged” 狀態日報表，偵測非納管設備



應用範例二：設備識別與資料統整

Collect

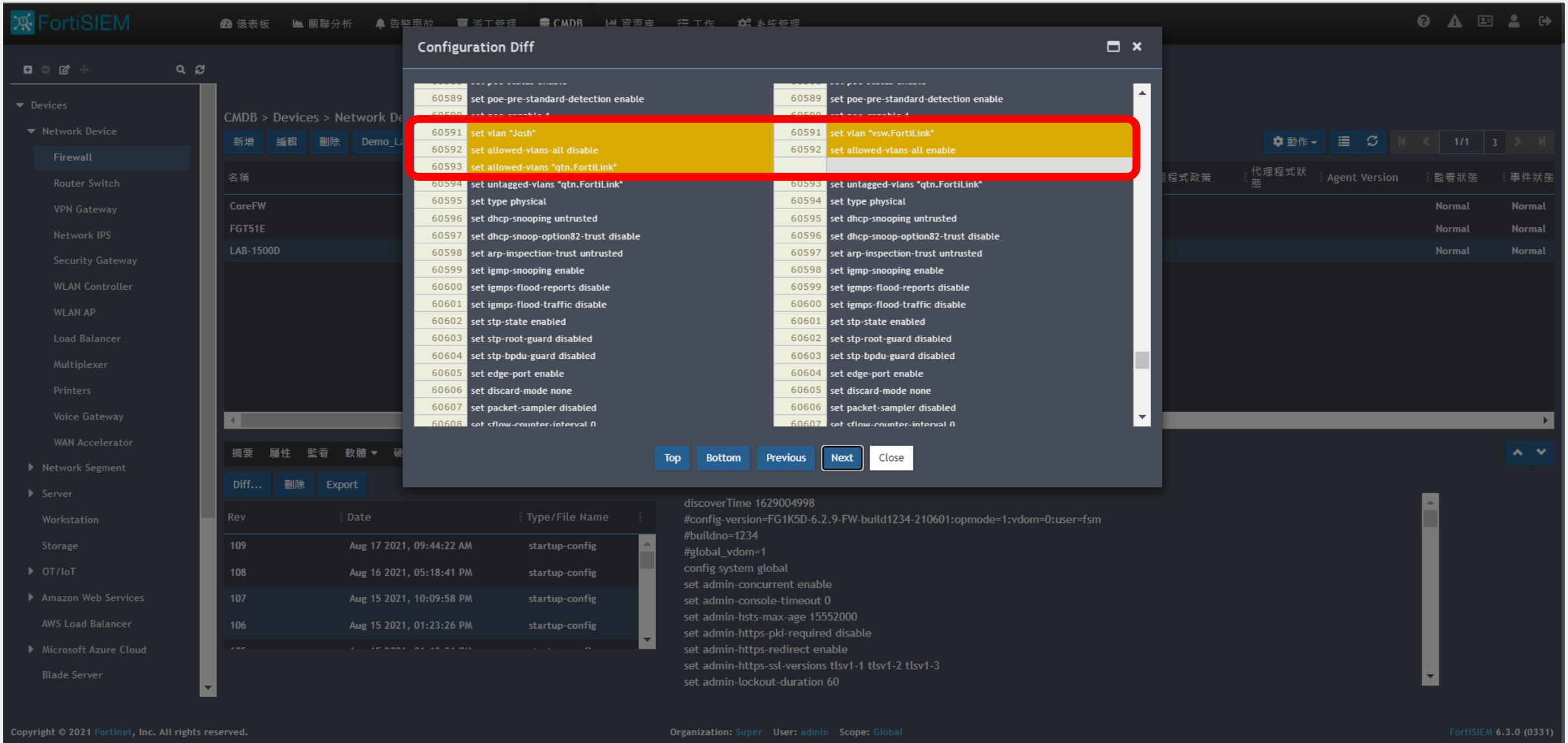
排程自動探索環境，身分、設備與連網位置自動關聯

- 透過排程自動探索環境 (L2 Scan)，更新 “Identity & Location” 儀表板，方便識別人員、設備與連線位置

應用範例三：設備識別與資料統整

Collect

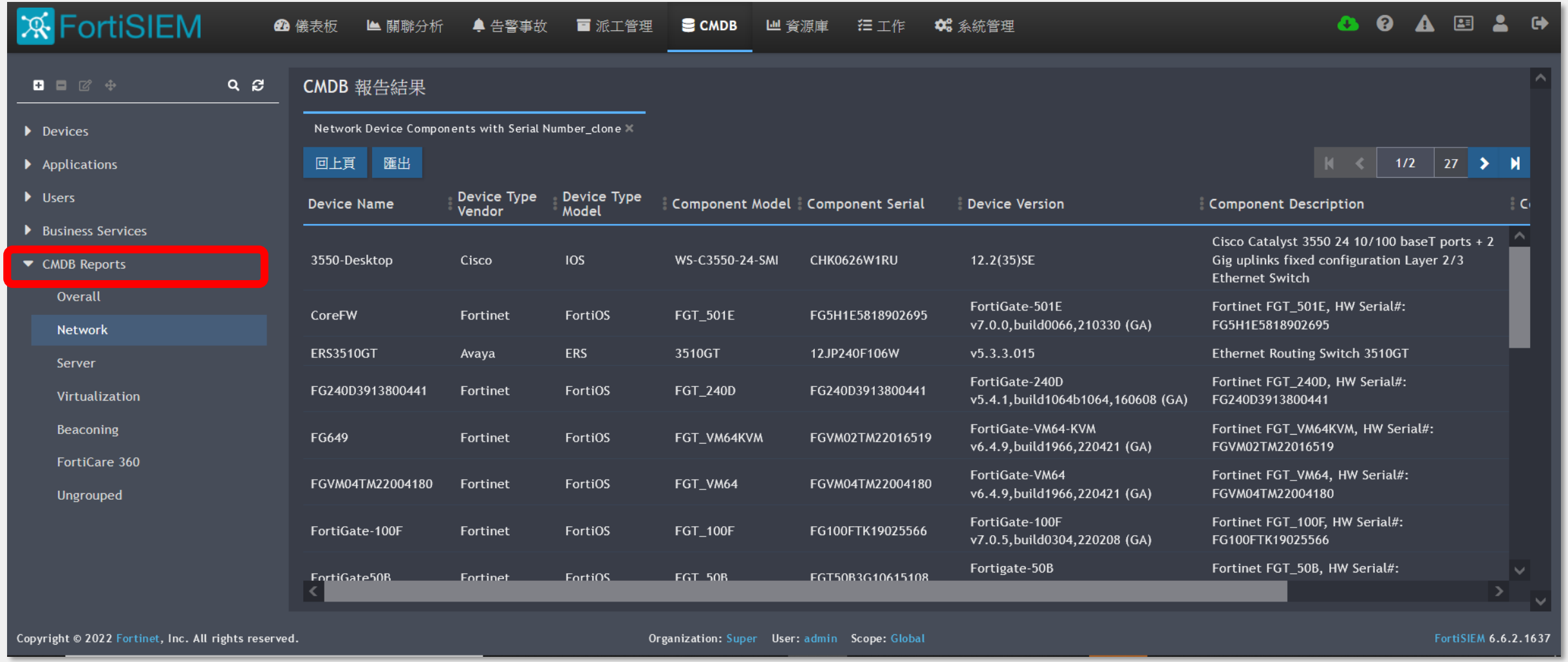
詳細檢視設備資訊、資安態勢、效能狀況、組態備份與異動比對



應用範例四：設備識別與資料統整

Collect

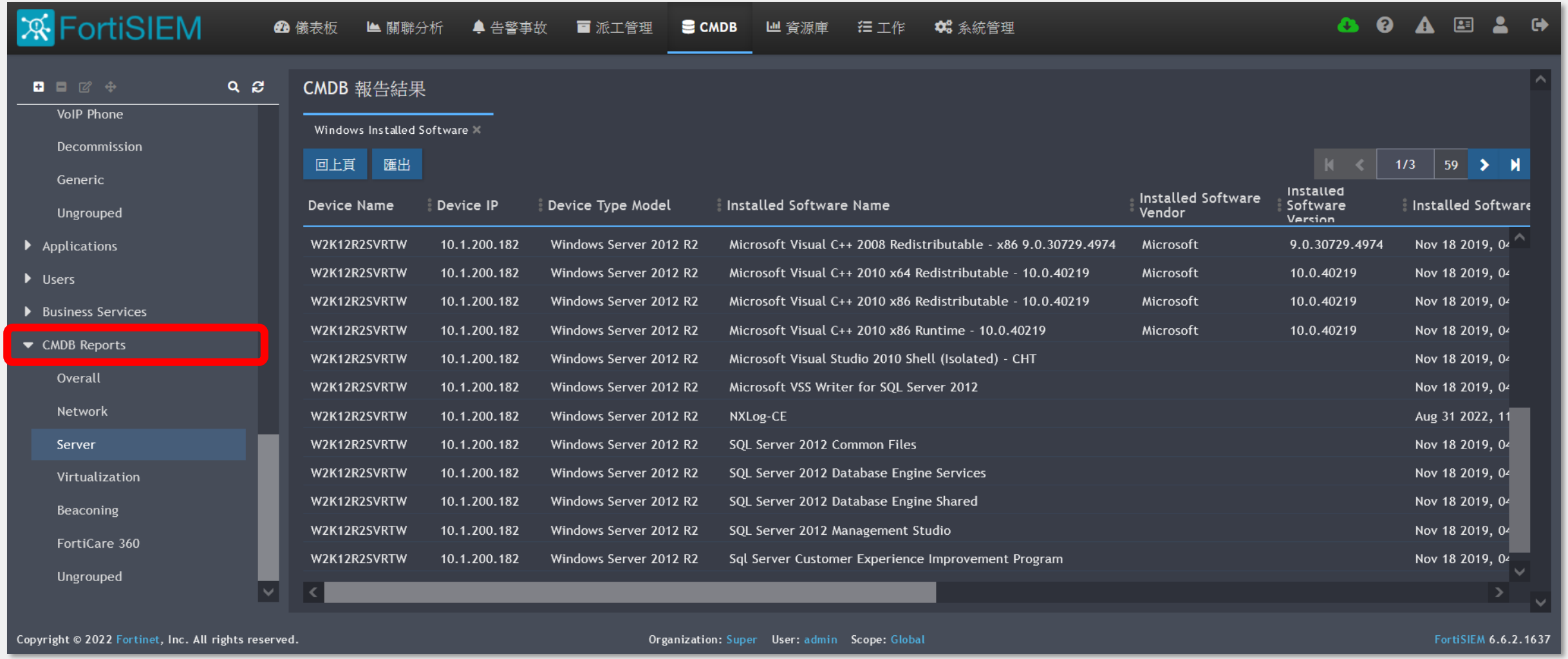
CMDB 設備資產盤點 (網路設備含序號資訊)



應用範例四：設備識別與資料統整

Collect

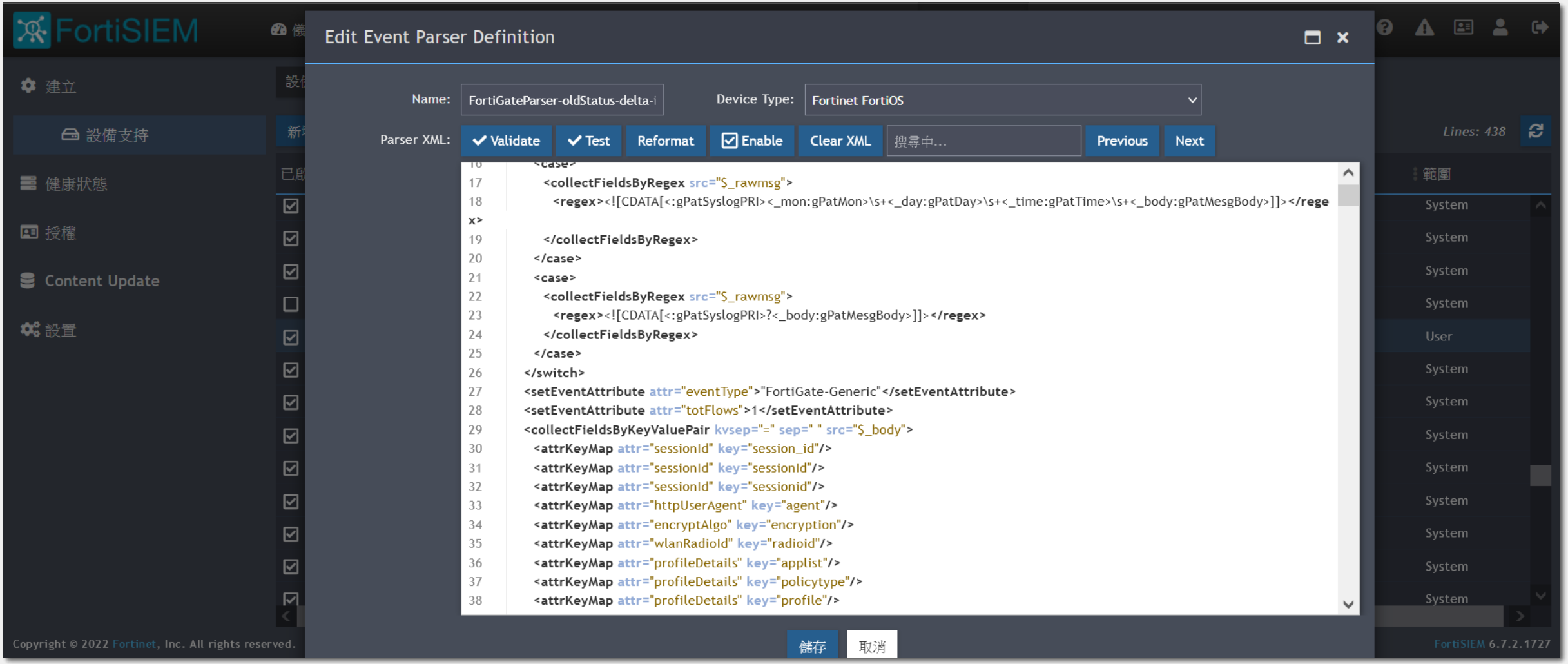
CMDB 設備資產盤點 (伺服器含安裝軟體資訊)



應用範例五：設備識別與資料統整

Collect

使用內建日誌解譯器編輯器 (Parser Editor) 調整正規化內容



威脅偵測 Detect

應用範例一：威脅與異常行為偵測

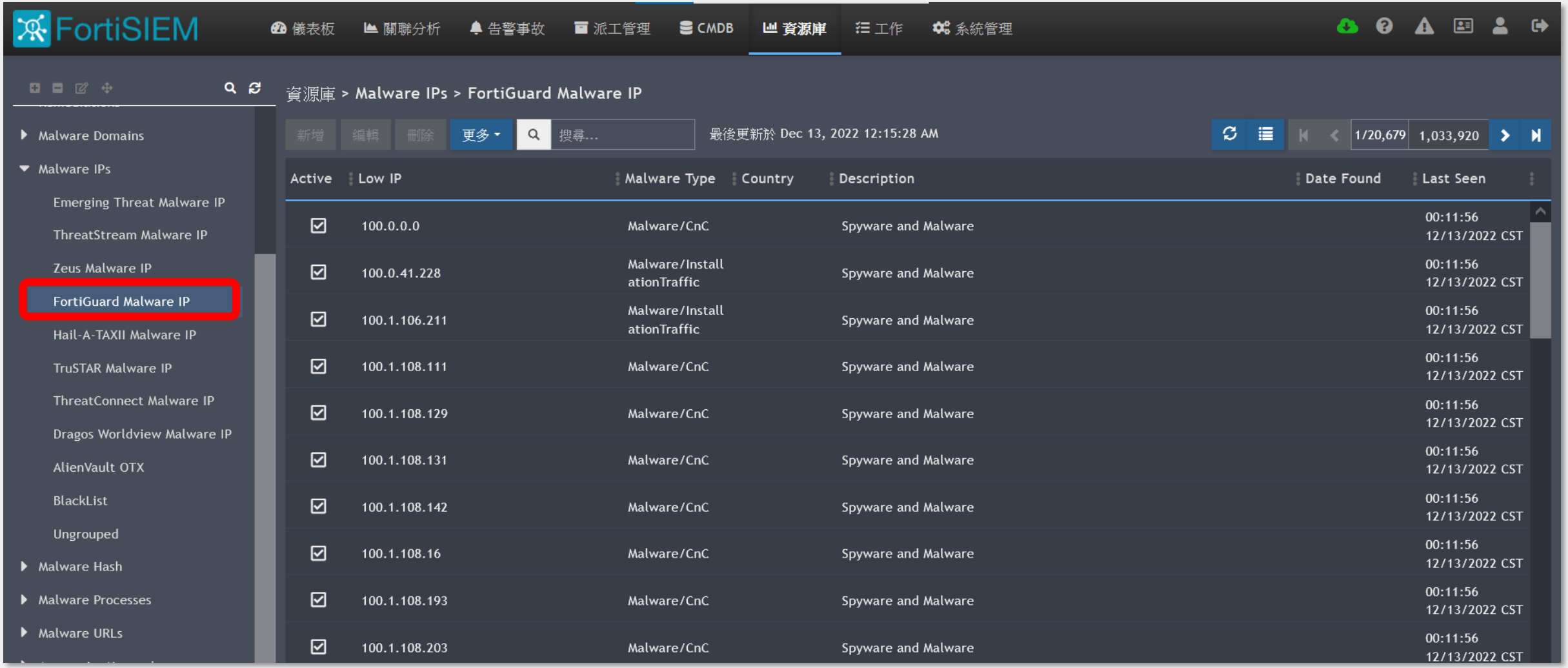
Detect

內建 AI / ML 關聯規則，協助建立營運基準線並偵測異常行為

應用範例二：威脅與異常行為偵測

Detect

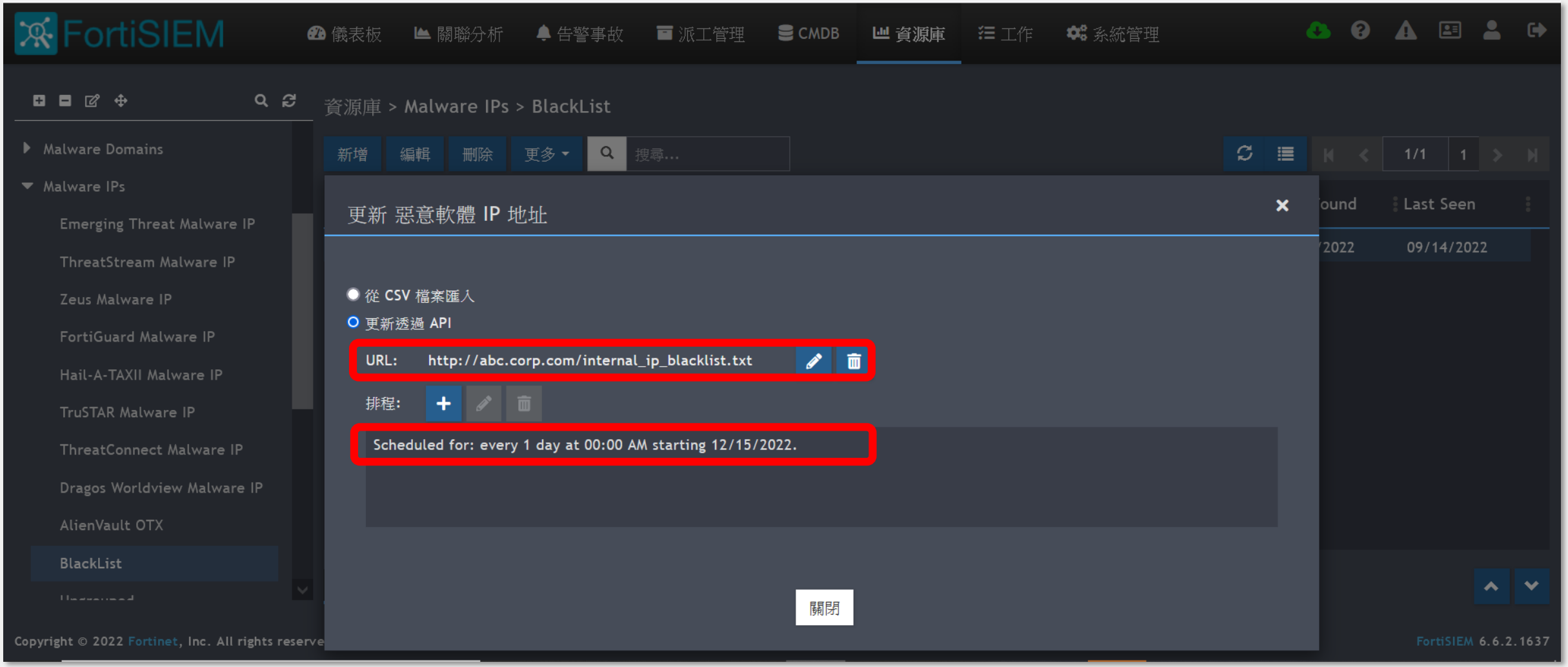
整合情資黑名單 (FortiGuard Lab)，快速發現可疑的對外連線



應用範例二：威脅與異常行為偵測

Detect

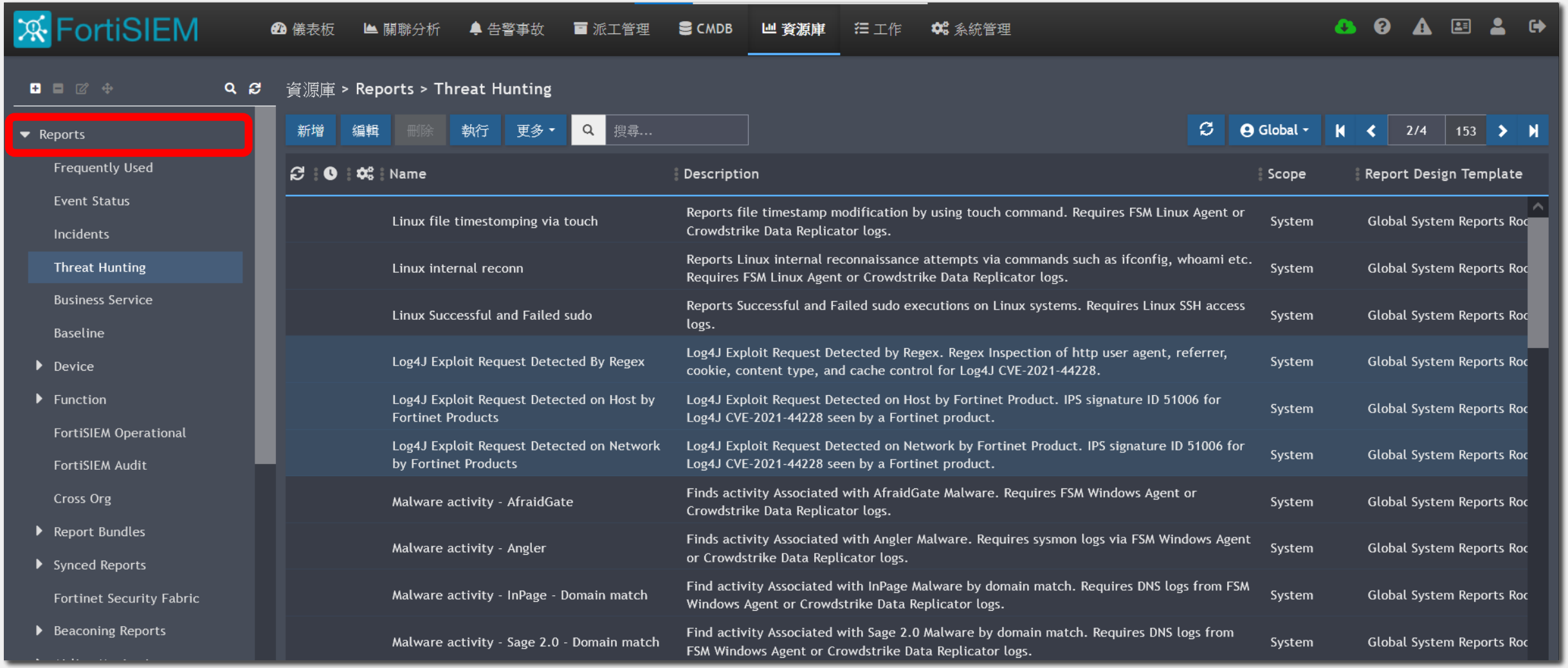
整合情資黑名單 (第三方或自行定義情資)，快速發現可疑的對外連線



應用範例三：威脅與異常行為偵測

Detect

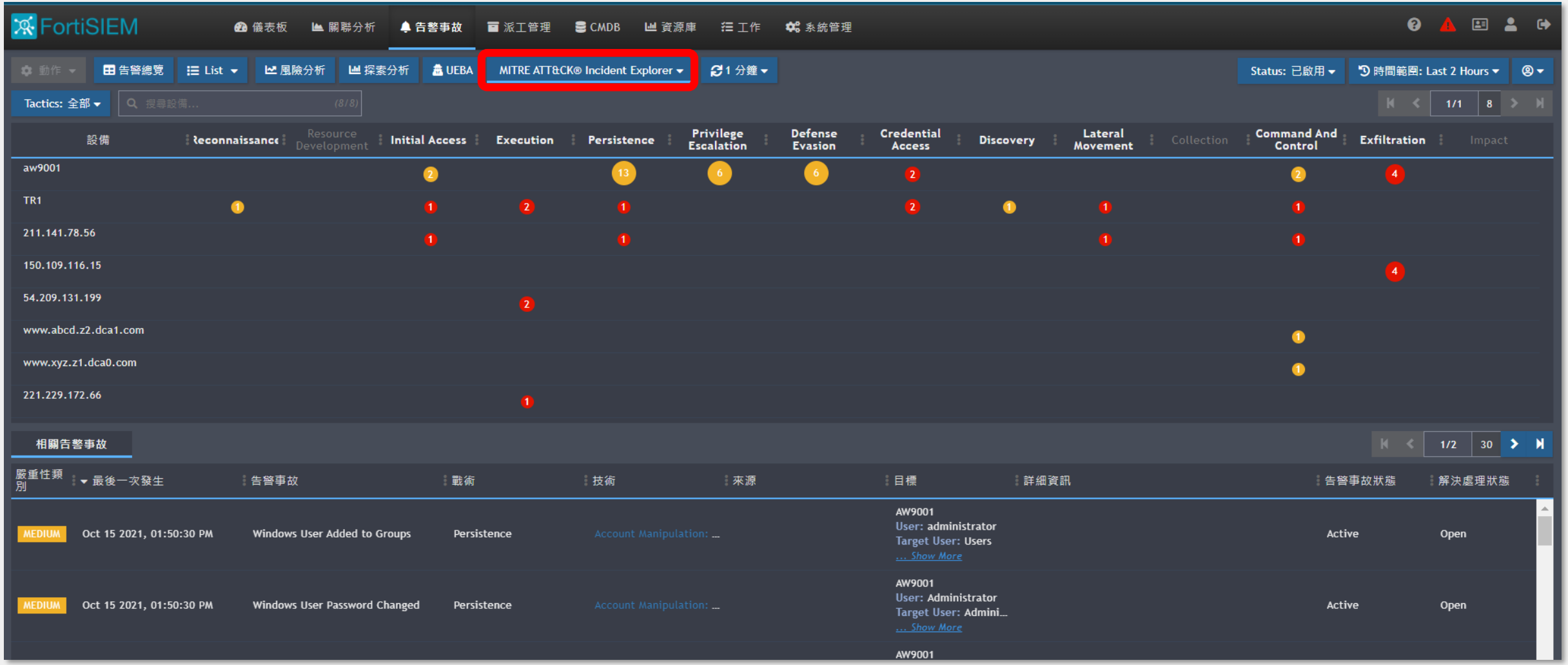
利用突發威脅告警相關之關聯規則、報表樣板，偵測、回溯及威脅獵捕可能的潛伏威脅



應用範例四：威脅與異常行為偵測

Detect

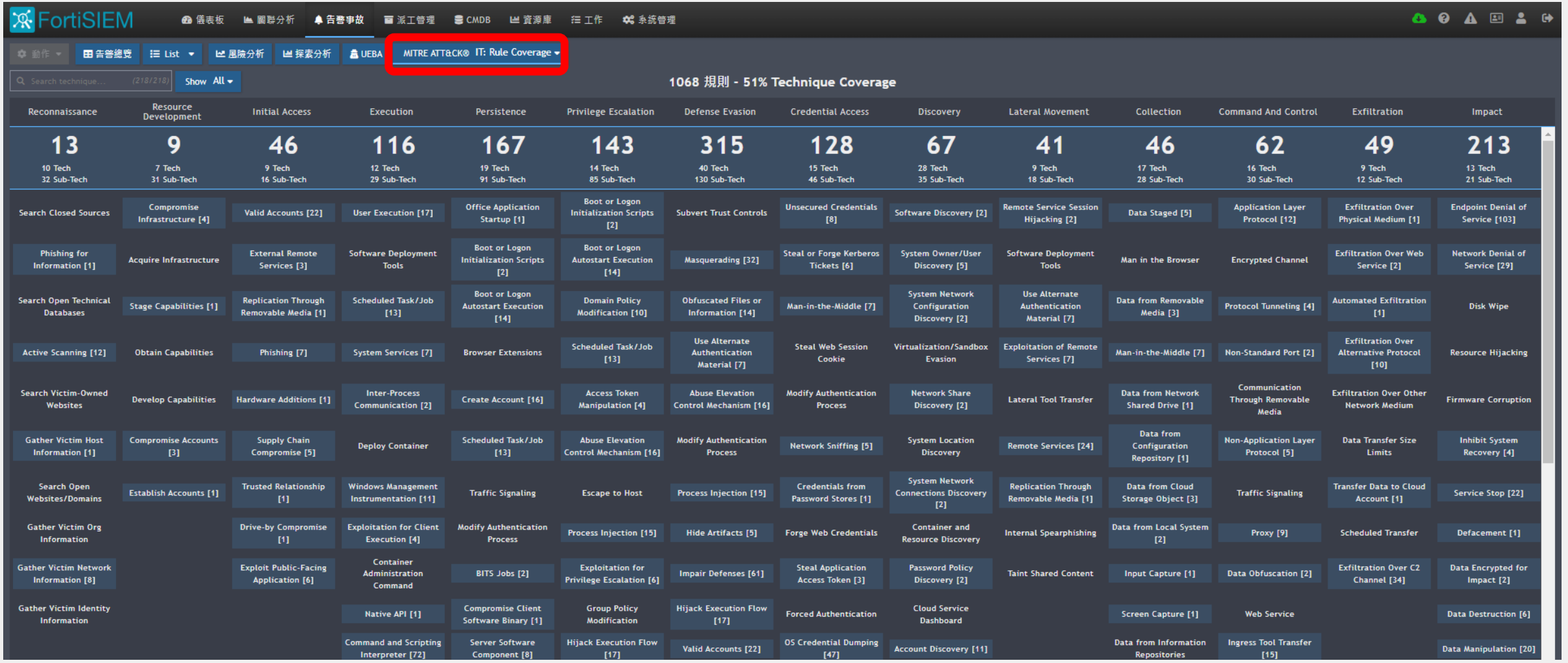
MITRE ATT&CK 資安對抗策略、手段告警圖，顯示進階持續性威脅 (Advanced Persistence Threat) 發生的各個階段



MITRE ATT&CK 資安對手策略、技術手法

關聯規則對應 MITRE ATT&CK 新資安框架 (Enterprise & ICS)

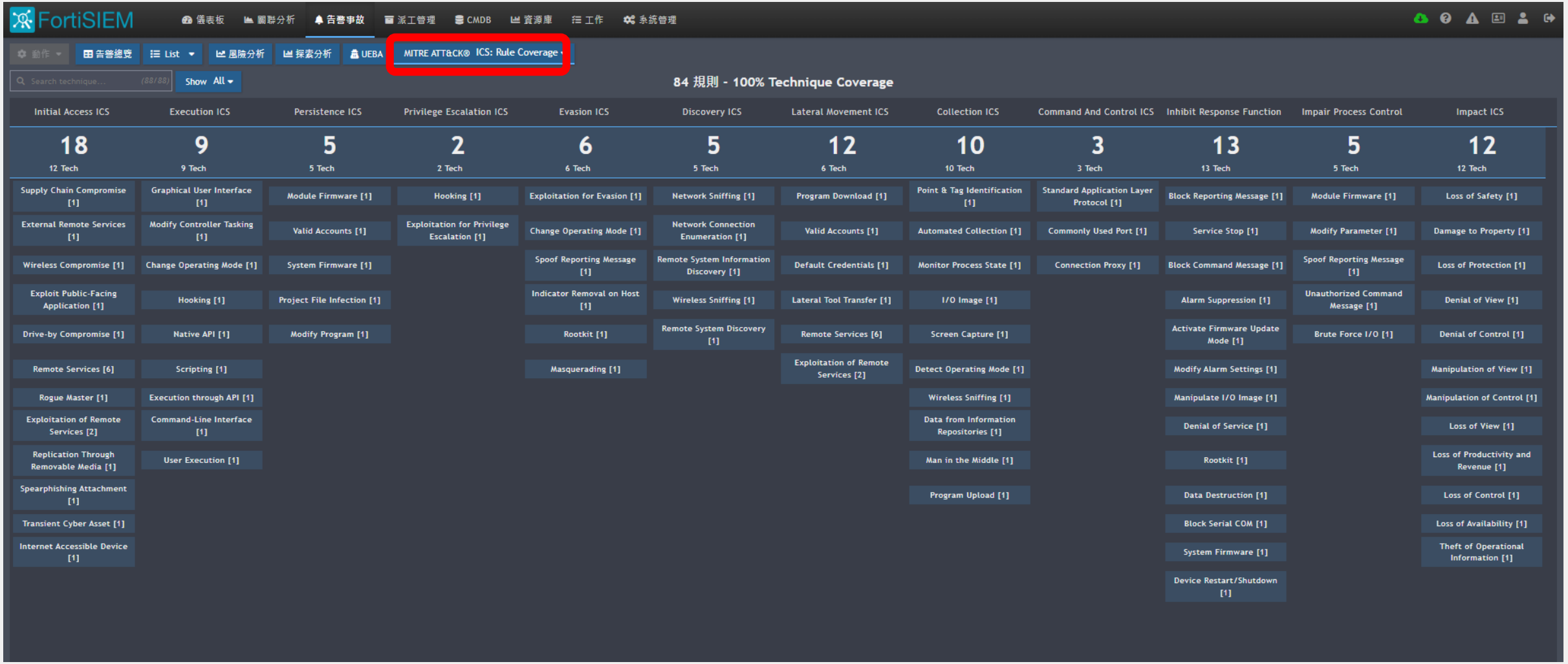
告警圖



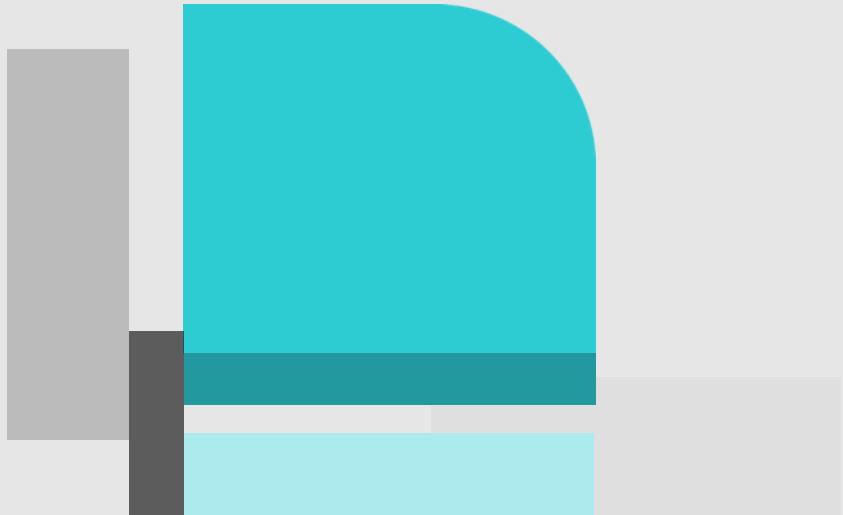
MITRE ATT&CK 資安對手策略、技術手法

關聯規則對應 MITRE ATT&CK 新資安框架 (Enterprise & ICS)

告警圖



維運監看 Monitor



應用範例一：維運監看 (告警總覽)

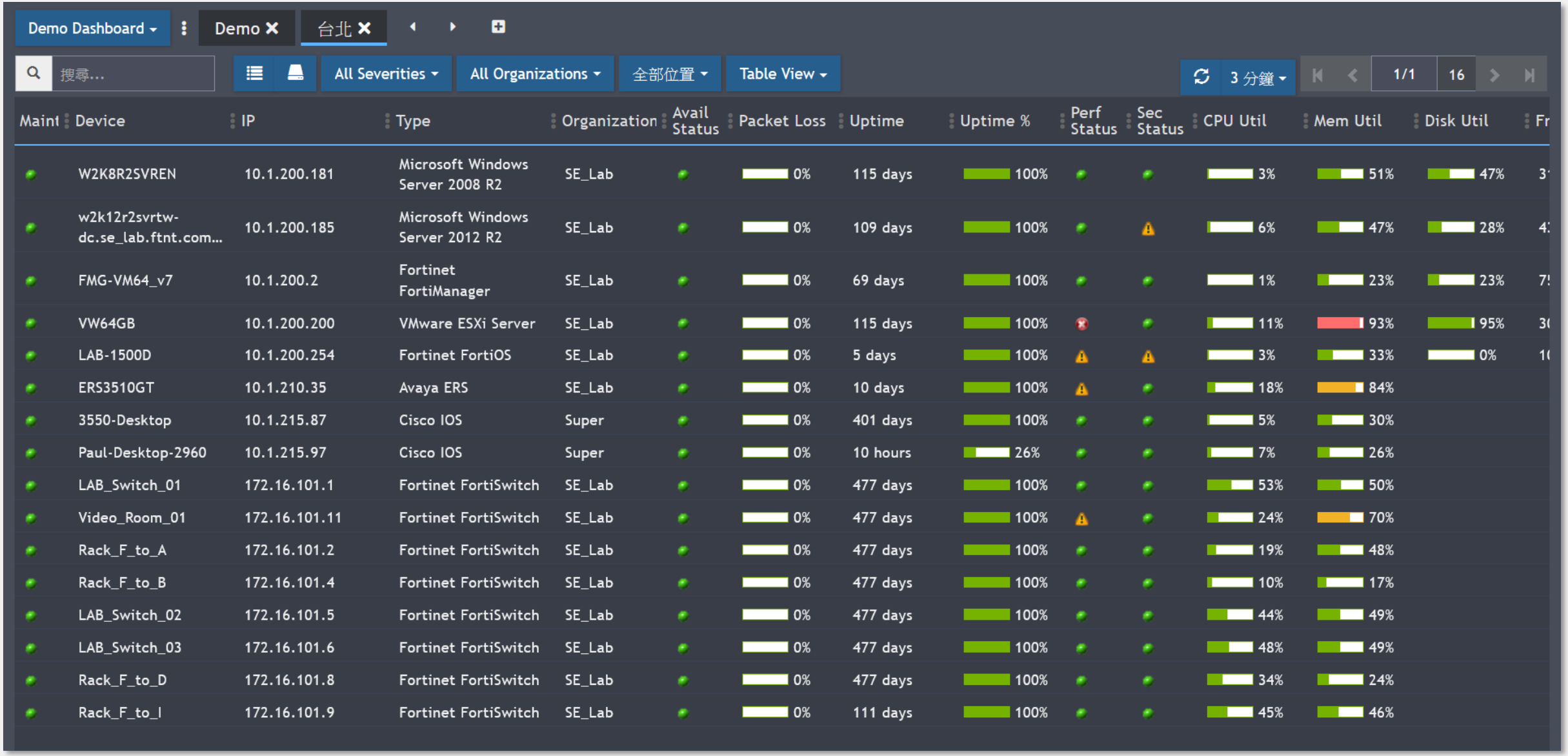
Monitor

所有告警事故分類、告警事故排行，受影響設備排行

應用範例二：維運監看 (設備一覽表)

Monitor

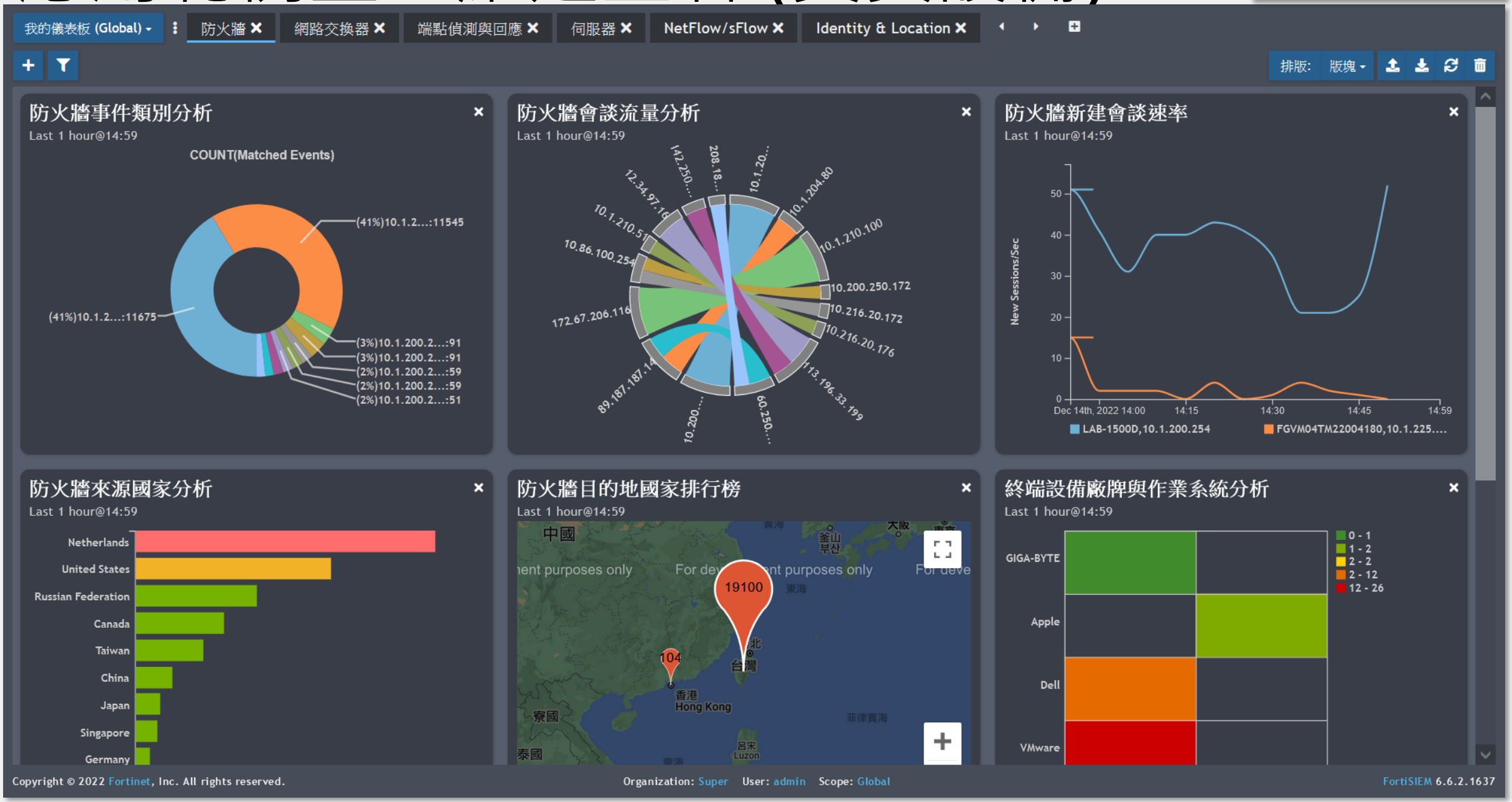
設備資安、效能、可用度一目瞭然



Maint	Device	IP	Type	Organization	Avail Status	Packet Loss	Uptime	Uptime %	Perf Status	Sec Status	CPU Util	Mem Util	Disk Util	Fr
	W2K8R2SVREN	10.1.200.181	Microsoft Windows Server 2008 R2	SE_Lab		0%	115 days	100%			3%	51%	47%	3
	w2k12r2svrtw-dc.se_lab.ftnt.com...	10.1.200.185	Microsoft Windows Server 2012 R2	SE_Lab		0%	109 days	100%			6%	47%	28%	4
	FMG-VM64_v7	10.1.200.2	Fortinet FortiManager	SE_Lab		0%	69 days	100%			1%	23%	23%	7
	VW64GB	10.1.200.200	VMware ESXi Server	SE_Lab		0%	115 days	100%			11%	93%	95%	3
	LAB-1500D	10.1.200.254	Fortinet FortiOS	SE_Lab		0%	5 days	100%			3%	33%	0%	1
	ERS3510GT	10.1.210.35	Avaya ERS	SE_Lab		0%	10 days	100%			18%	84%		
	3550-Desktop	10.1.215.87	Cisco IOS	Super		0%	401 days	100%			5%	30%		
	Paul-Desktop-2960	10.1.215.97	Cisco IOS	Super		0%	10 hours	26%			7%	26%		
	LAB_Switch_01	172.16.101.1	Fortinet FortiSwitch	SE_Lab		0%	477 days	100%			53%	50%		
	Video_Room_01	172.16.101.11	Fortinet FortiSwitch	SE_Lab		0%	477 days	100%			24%	70%		
	Rack_F_to_A	172.16.101.2	Fortinet FortiSwitch	SE_Lab		0%	477 days	100%			19%	48%		
	Rack_F_to_B	172.16.101.4	Fortinet FortiSwitch	SE_Lab		0%	477 days	100%			10%	17%		
	LAB_Switch_02	172.16.101.5	Fortinet FortiSwitch	SE_Lab		0%	477 days	100%			44%	49%		
	LAB_Switch_03	172.16.101.6	Fortinet FortiSwitch	SE_Lab		0%	477 days	100%			48%	49%		
	Rack_F_to_D	172.16.101.8	Fortinet FortiSwitch	SE_Lab		0%	477 days	100%			34%	24%		
	Rack_F_to_I	172.16.101.9	Fortinet FortiSwitch	SE_Lab		0%	111 days	100%			45%	46%		

應用範例三：維運監看 (資安設備)

Monitor



Organization: Super User: admin Scope: Global

FortiSIEM 6.6.2.1637

應用範例四：維運監看 (網路設備)

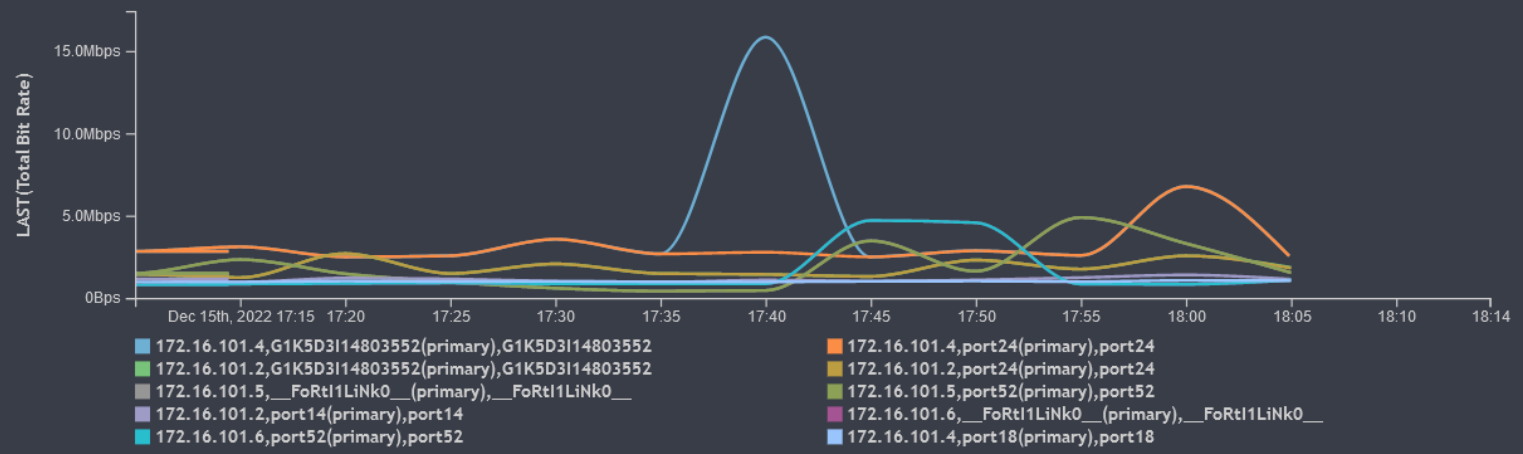
Monitor

我的儀表板 (Global) | 防火牆 | 網路交換器 | 端點偵測與回應 | 伺服器 | NetFlow/sFlow | Identity & Location

排版: 版塊

網路交換器介面流量分析

Last 1 hour@18:14



網路交換器系統資源用量分析 (CPU Util)

Last 1 hour@18:14

Reporting IP	LAST(CPU Util)	Trend
172.16.0.4	63%	
172.16.101.6	44%	
172.16.101.5	36%	
172.16.101.9	34%	
192.168.19.1	34%	
172.16.101.1	31%	
172.16.101.11	27%	

網路交換器登入成功/失敗

Last 1 hour@18:15

ve Time	Reporting Device	Reporting IP	User	Source IP	Method	Status
05:59:32 PM	Video_Room_01	172.16.101.11	jim	10.1.210.100	ssh	failed
05:59:31 PM	Video_Room_01	172.16.101.11	jim	10.1.210.100	ssh	failed
05:59:24 PM	Video_Room_01	172.16.101.11	jim	10.1.210.100	ssh	failed
05:58:32 PM	Video_Room_01	172.16.101.11	admin	10.1.210.100	https	success
05:57:57 PM	Video_Room_01	172.16.101.11	admin	10.1.210.100	ssh	success
05:54:37 PM	Video_Room_01	172.16.101.11	fsm	10.1.210.100	https	success

網路交換器系統資源用量分析 MAX(Memory ...

Last 1 hour@18:14

Reporting IP	MAX(Memory Util)	Trend
10.1.210.35	83.59%	
172.16.101.11	70.74%	
172.16.0.4	51%	
172.16.101.1	50.11%	
172.16.101.6	48.95%	
172.16.101.5	48.85%	

Organization: Super User: admin Scope: Global

FortiSIEM 6.6.2.1637

應用範例五：維運監看 (端點安全)

Monitor

我的儀表板 (Global) | 防火牆 | 網路交換器 | 端點偵測與回應 | 伺服器 | NetFlow/sFlow | Identity & Location

排版: 版塊

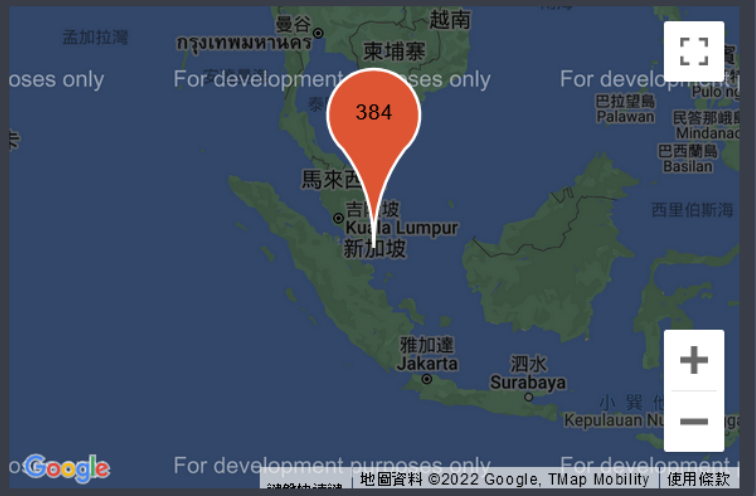
安全事件統計 (依規則)

Last 8 hours@15:09

Event Name	Firewall Action	Rule Name	COUNT(Matched Events)
FortiEDR blocked inconclusive file	Blocked (Simulation)	Dynamic Code - Malicious Runtim...	9216
FortiEDR blocked suspicious file	Blocked (Simulation)	Dynamic Code - Malicious Runtim...	5056
FortiEDR-Security-PUP-Logged	Logged	Unconfirmed File Detected	1152
FortiEDR blocked malicious file	Blocked (Simulation)	Malicious File Detected	1088
FortiEDR blocked suspicious file	Blocked	Dynamic Code - Malicious Runtim...	384
FortiEDR-Security-FortiEDR-Syslog-message-FortiEDR-Sy...	FortiEDR Syslog message		256
FortiEDR blocked malicious file	Blocked (Simulation)	Unconfirmed Executable - Execut...	192
FortiEDR-Security-PUP-Blocked	Blocked (Simulation)	Malicious File Detected	192
FortiEDR blocked suspicious file	Blocked	Suspicious Application - Connecti	128

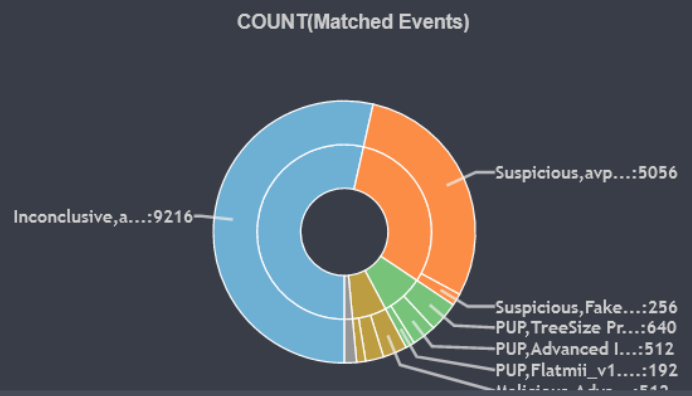
資安事件外部IP統計

Last 8 hours@15:09



可疑應用程式統計

Last 8 hours@15:09



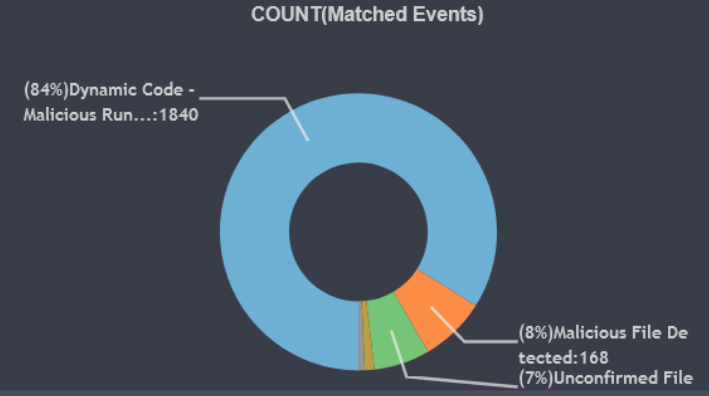
惡意檔案統計 (依來源)

Last 8 hours@15:09

Source IP	File Name	COUNT(Matched Events)
192.168.1.155	avp.exe	14k
10.1.1.8	Advanced IP Address ...	512
10.1.1.8	Advanced Port Scann...	512
10.1.1.8	TreeSize Professional...	512
10.1.1.8	keygen.exe	384
192.168.1.69	Fake Minecraft Instal...	256
192.168.1.155	Flatmii_v1.5.exe	192

規則使用排行榜

Last 1 hour@15:09



Organization: Super User: admin Scope: Global

FortiSIEM 6.6.2.1637

應用範例六：維運監看 (主機設備)

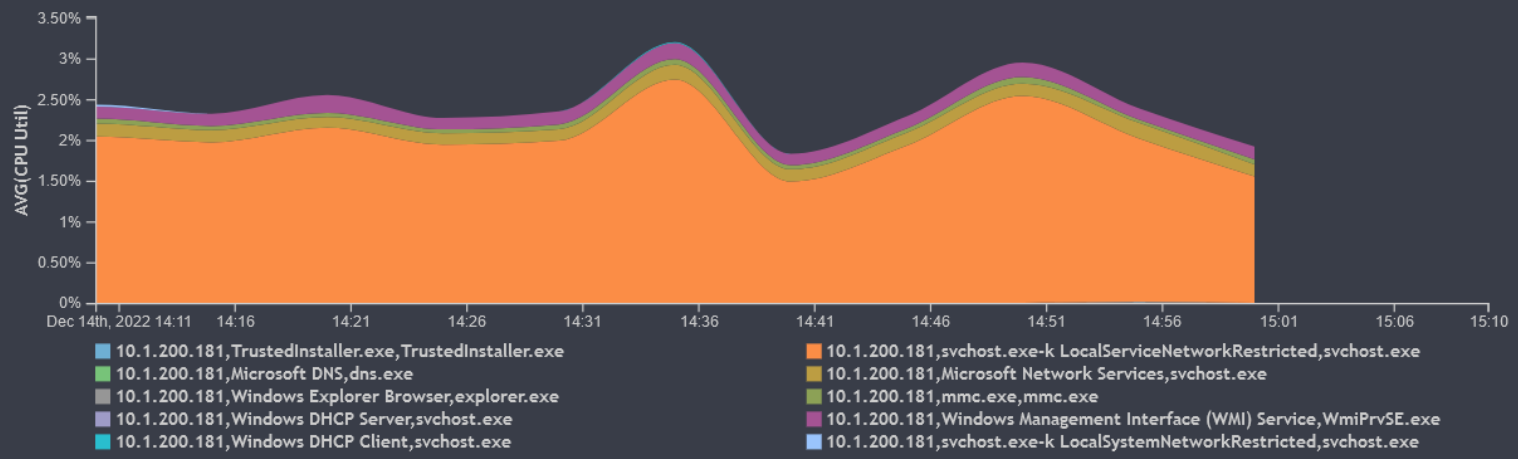
Monitor

我的儀表板 (Global) | 防火牆 | 網路交換器 | 端點偵測與回應 | 伺服器 | NetFlow/sFlow | Identity & Location

排版: 版塊

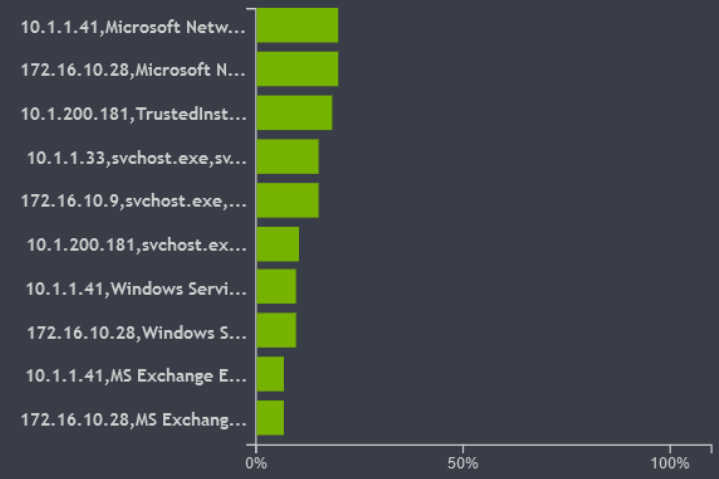
Windows 程式CPU資源使用率分析 (平均值)

Last 1 hour@15:10



Windows 程式記憶體資源使用率分析 (最大值)

Last 1 hour@15:10



Windows登入失敗記錄

Last 1 hour@15:10

Event Receive Time	User	Server
Dec 14 2022, 02:34:27 PM	matt	W2K8R2SVRTW
Dec 14 2022, 02:34:27 PM	kevin	W2K8R2SVREN
Dec 14 2022, 02:34:27 PM	jim	W2K8R2SVRTW
Dec 14 2022, 02:34:26 PM	kevin	W2K8R2SVREN
Dec 14 2022, 02:34:26 PM	vincent	W2K8R2SVREN
Dec 14 2022, 02:34:26 PM	vincent	W2K8R2SVREN

Windows檔案異動記錄

Last 1 hour@15:10

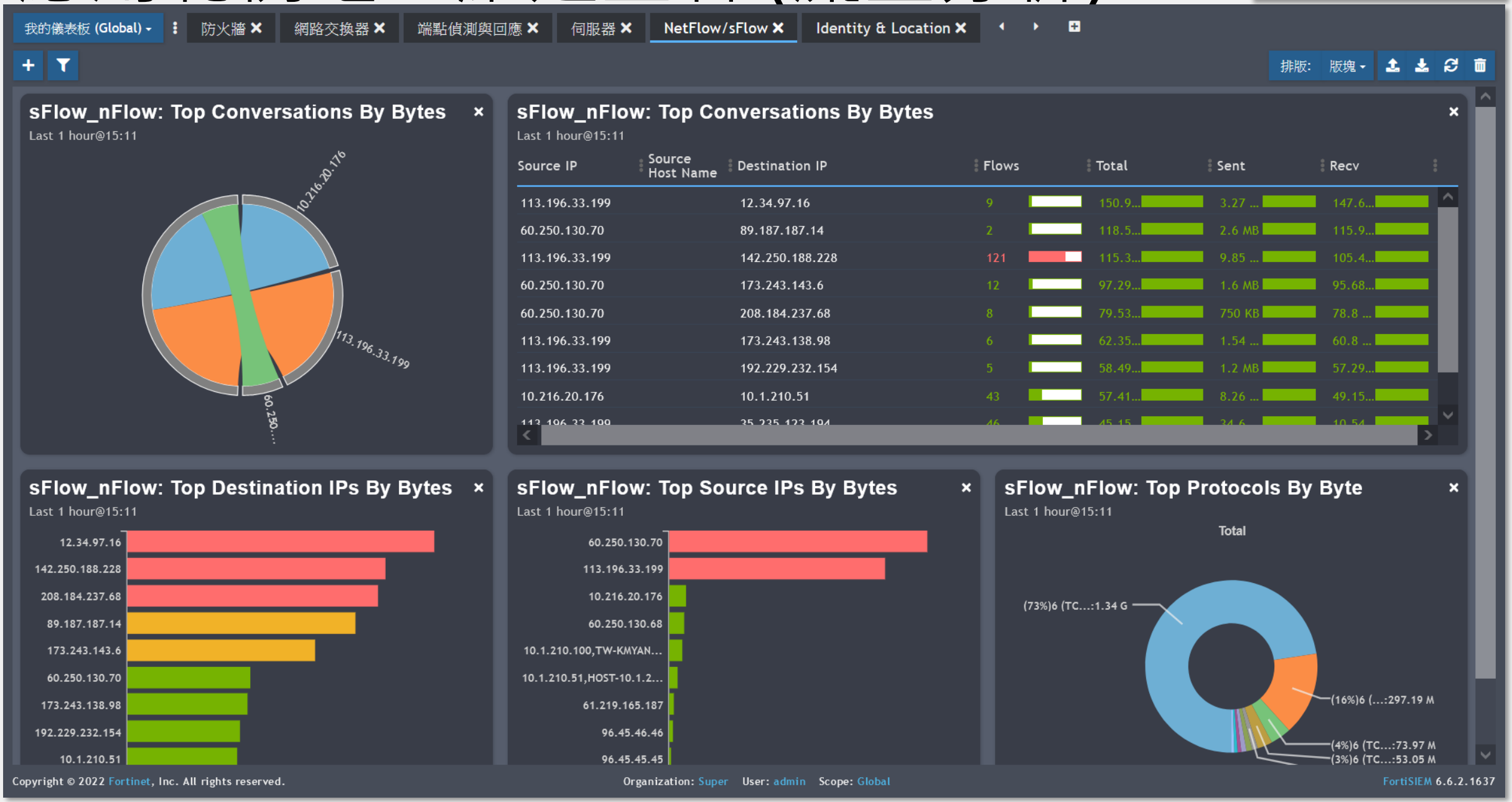
Event Receive Time	Server	User	Action	File Name
Dec 14 2022, 02:34:26 PM	W2K8R2SVREN	summer	Modified	c:\zone\新產品發表計畫書.txt
Dec 14 2022, 02:34:26 PM	W2K8R2SVREN	gary	Modified	c:\zone\員工薪資查核表.rtf
Dec 14 2022, 02:34:26 PM	W2K8R2SVREN	lily	Added	c:\zone\New Rich Text Document.rtf
Dec 14 2022, 02:34:26 PM	W2K8R2SVREN	gary	Removed	c:\zone\十月內部稽核會議記錄.txt
Dec 14 2022, 02:34:26 PM	W2K8R2SVREN	gary	Removed	c:\zone\九月內部稽核會議記錄.txt
Dec 14 2022, 02:34:25 PM	W2K8R2SVREN	gary	Modified	c:\zone\公司Q1財報會議記錄.rtf
Dec 14 2022, 02:34:25 PM	W2K8R2SVREN	gary	Modified	c:\zone\員工通訊錄.txt

Organization: Super User: admin Scope: Global

FortiSIEM 6.6.2.1637

應用範例七：維運監看 (流量分析)

Monitor

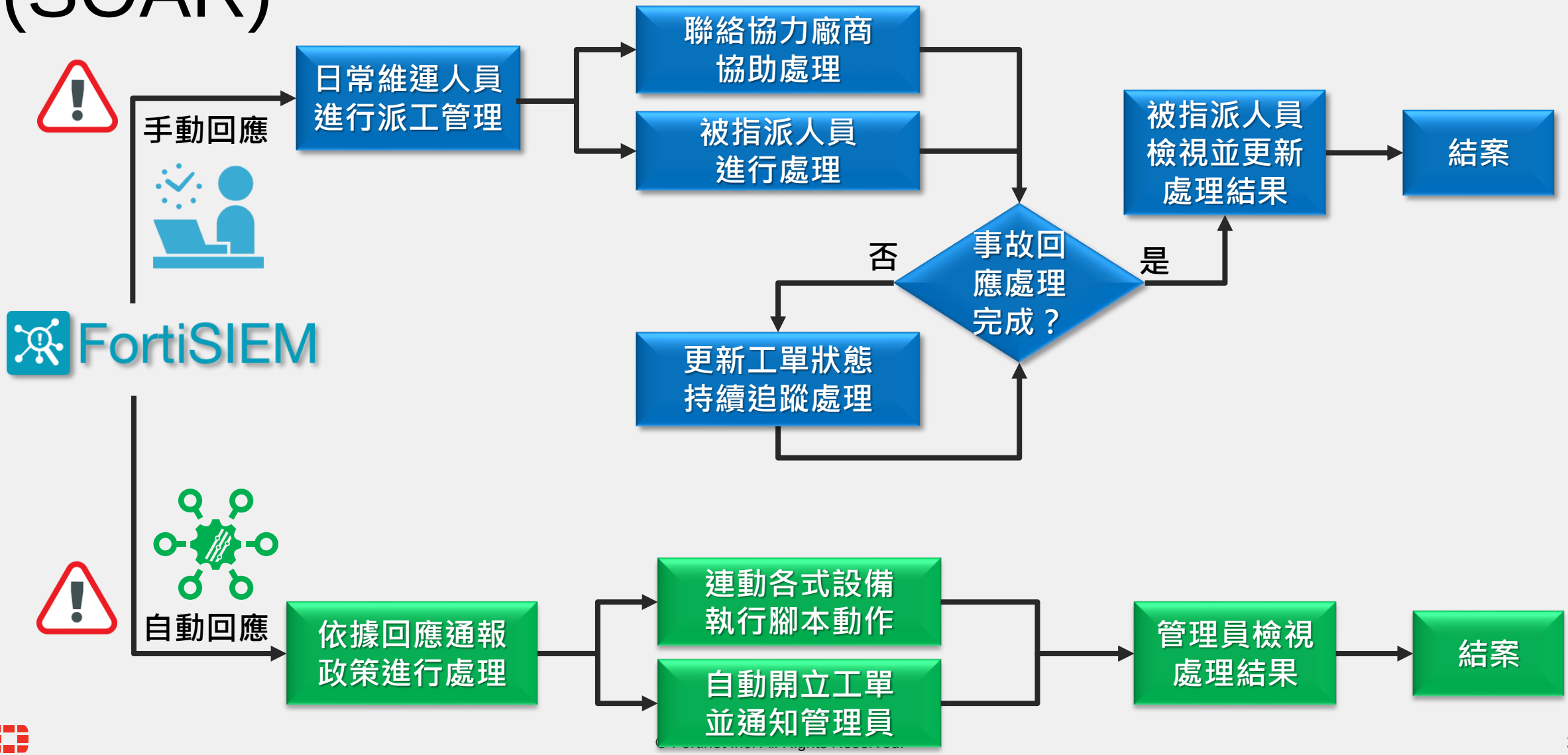


事故回應 Respond

應用範例一：告警事故協作回應與自動化 (SOAR)

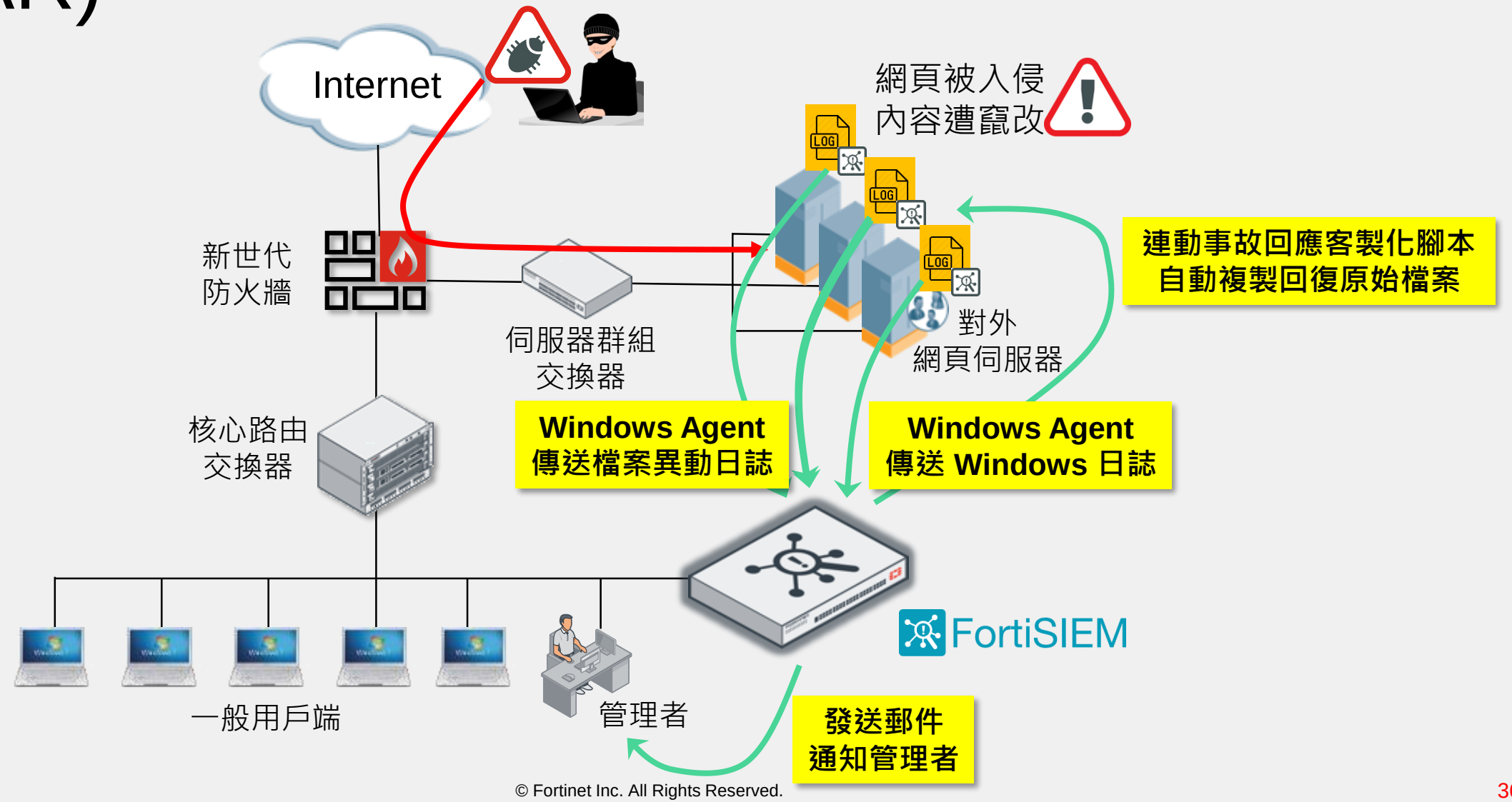
Respond

手動與自動化告警事故回應流程



應用範例二：告警事故協作回應與自動化 Respond (SOAR)

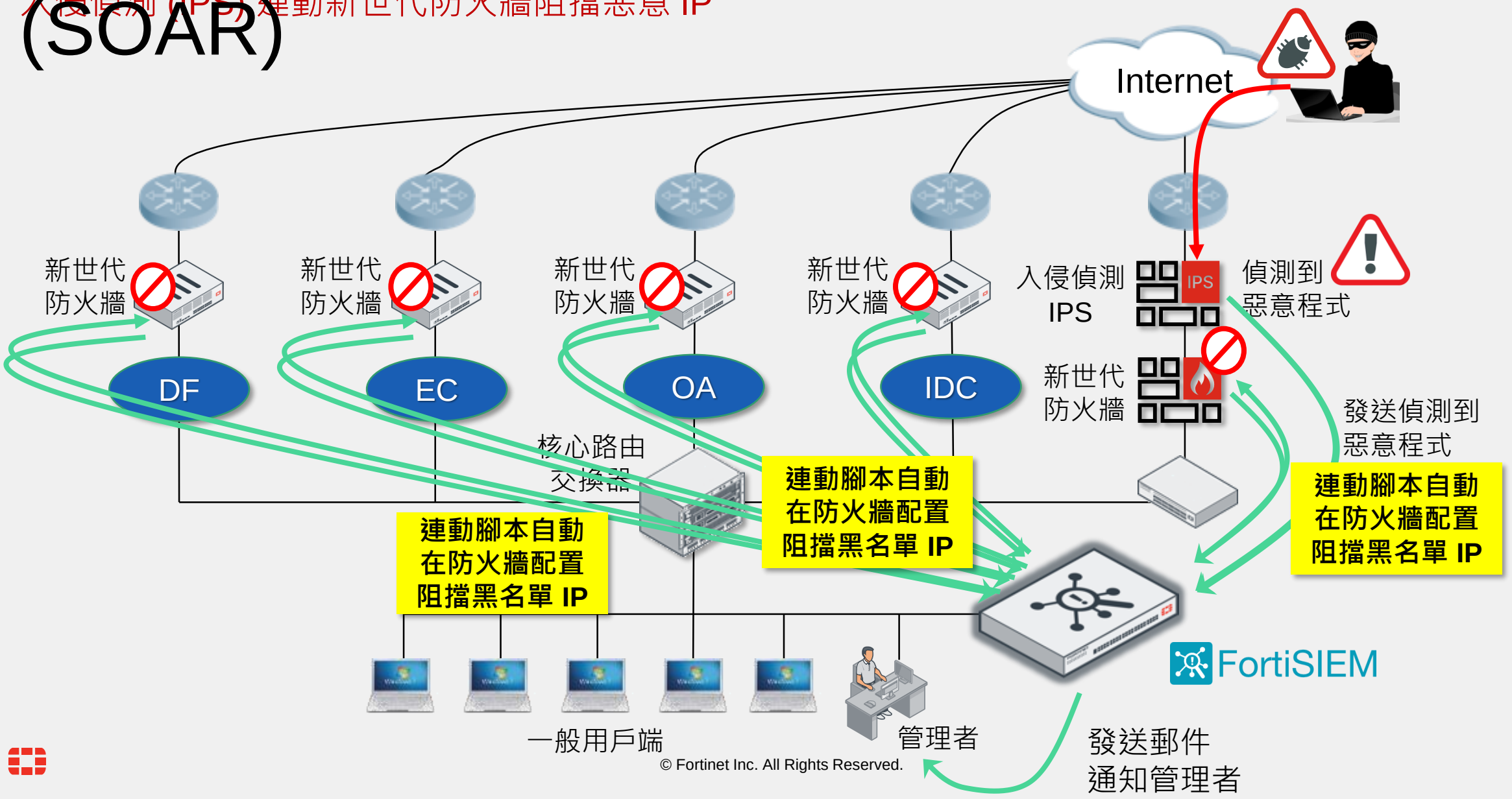
檔案異動偵測連動網頁竄改復原機制



應用範例三：告警事故協作回應與自動化 (SOAR)

Respond

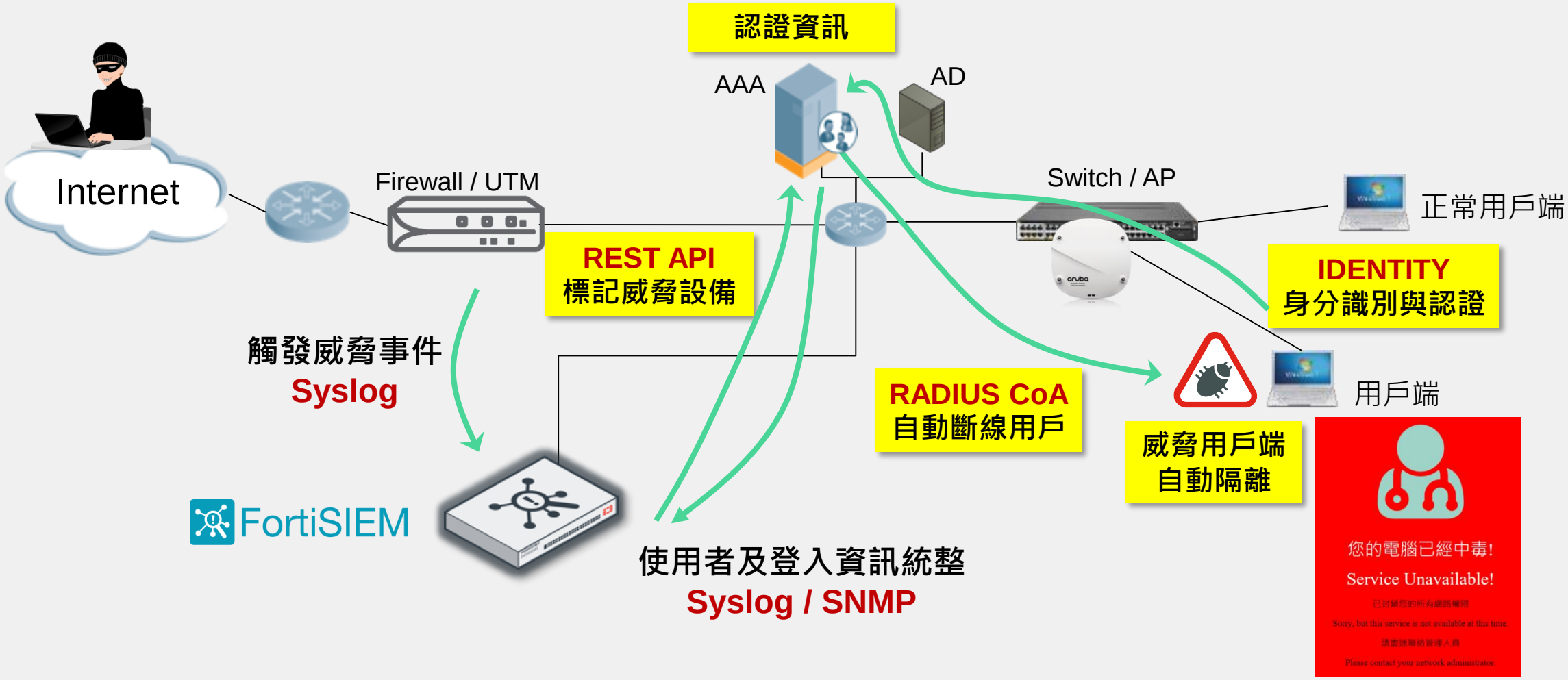
入侵偵測 (IPS) 連動新世代防火牆阻擋惡意 IP



應用範例四：告警事故協作回應與自動化 (SOAR)

Respond

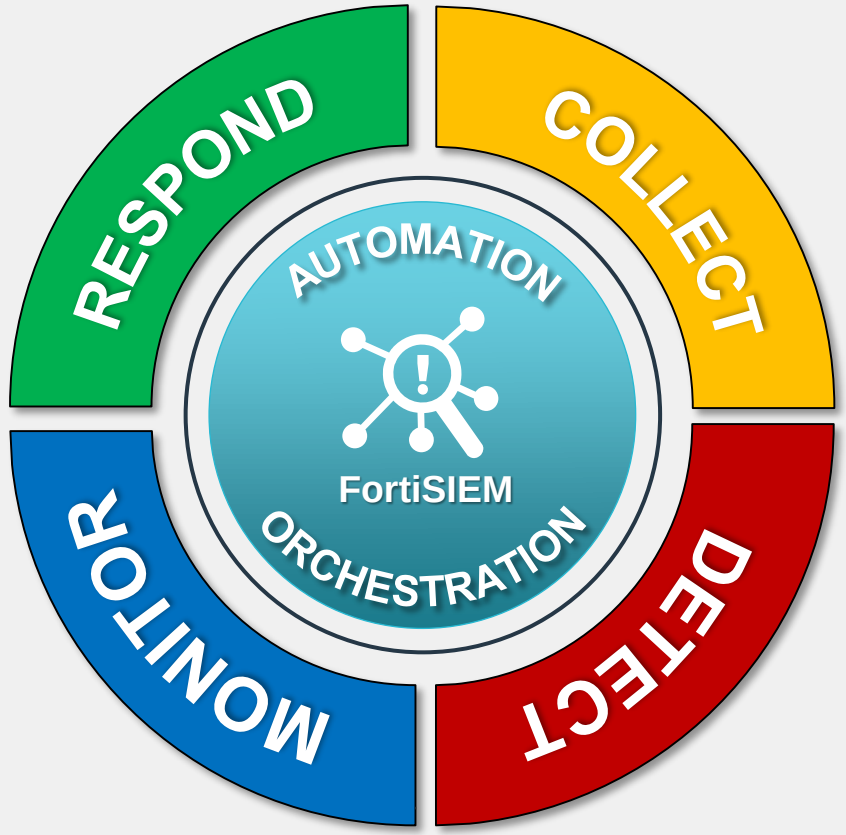
使用者 (有線/無線) 入網異常行為監看與自動隔離



FortiSIEM 重要特點與價值

資料統整、威脅偵測、維運監看、事故回應一氣呵成

- 各種資訊匯集統整，日誌稽核，合規報表，安全資訊與事件管理 (SIEM)
- 還可以作為資安/網維管理的優化工具
- AI / ML 智能關聯分析，對應 MITRE 資安框架，提供威脅先期預警能力
- 彈性的資安/網維儀表板提供更好可視性
- 內建派工管理，連動跨品牌的設備，滿足協作聯防、自動化回應 (SOAR) 需求




親愛的老師們，感謝您即將使用 FortiSIEM
新世代 SIEM 平台


您決定使用 FortiSIEM 的一小步，
是您校園資訊安全進程的一大步


FORTINET